Analytic enumeration of isomorphic classes of binary linear codes according with Marcel Wild research.

By Alexander Erick Trofimoff

Graduate Research Assistant

PhD program Drexel U.

ECE dept fall 2014

Bibliography

- Brilawski T, Lucas D, Uniquely representable combinatorial geometries, 1973
- Wild M., The Asymptotic number of inequivalent Binary codes and nonisomorphic binary matroids, May 1999
- Wild M., Consequences of the Brylawski-Lucas Th. for binary matroids, 1996
- Wild M, Enumeration of binary and Ternary Matroids and other applications of the Brylawski-Lucas Theorem, Preprint, 1994
- Kung J. , The cycle structure of linear Transformation over a finite field, 1981.
- Kerber A., Applied Finite Group actions, Springer 1991
- Kerber A., Algebraic Combinatorics via Finite group actions 1991
- Dummit, D., Foote R., Abstract Algebra

Outline of Presentation

- ✓ Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Row, Projective and Geometric equivalence among matrix representations

Definition: (Projective operation)

- Add scalar multiple of a row to another
- Permuting 2 rows
- Multiply a row by a scalar ($\neq 0$)

$M \underset{\sim}{R} M'$

$M \underset{\sim}{P} M'$

- elementary row operation,
- multiplication of a column by nonzero scalar,
- a removal of a zero row.

Definition: (Geometrically equivalent Matrices)

projective operation does not affect column dependence,

matrices

M ⟷ M'

differ by a series of projective operations

$M \underset{\sim}{P} M'$

⇓

represent same pregeometry (Matroid).

$M \underset{\sim}{G} M'$

$M \underset{\sim}{R} M' \rightarrow M \underset{\sim}{P} M \rightarrow M \underset{\sim}{G} M'$

Projective equivalence in between matrix representations

$$\mathrm{M} \underset{\sim}{^{P}} \mathrm{M'}$$

Definition: (Projectively equivalent matrices)

Two matrices

projectively

equivalent

if

$M' = NMD,$

N

nonsingular $r \times r$

matrix

D

nonsingular

$n \times n$ diagonal

matrix.

Number of distinct matrix representations under Projective equivalence

Proposition:

Let G be a matroid (pregeometry)

rank r   cardinality n,

k connected components.

P coordinatizing path of A

If $M = IA$

represents G over F

$if \mid F \mid = q,$

$\exists$

$(q-I)^{n-k}$ distinct matrices

$[IA'] = M' \overset{P}{\sim} M$

$\exists$

$(q^r - I)(q^r - q)\ldots(q^r - q^{r-1})(q-I)^{n-k}$

distinct $r \times n$ matrices,

$PA' = M' \overset{P}{\sim} M$

Number of matrices and equivalence classes under row equivalence

Corollary:

If G representable over F, $|F| = q$,

each projective equivalence class

with

PA' $r \times n$ representations

is partioned into

$(q-I)^{n-k}$ distinct row equivalence classes

each class contains $\prod_{i=0,r-1} q^r - q^i$

$r \times r$ non singular distinct matrices over F_q.

Closure operator

Definition: Closure operator is the mapping $c : 2^E \to 2^E$

A **closure operator** on a set S $\mathrm{cl} : \mathcal{P}(S) \to \mathcal{P}(S)$

$X, Y \subseteq S$

(Preservation of Nullary Union) $c(\varnothing) = \varnothing$

(cl is *extensive*) $X \subseteq c(X)$

(cl is *increasing*) $X \subseteq Y \Rightarrow c(X) \subseteq c(Y)$

(cl is *idempotent*) $c(c(X)) = c(X)$

Kuratowski axioms

(E,c) is called closure space.

Closure as a generalization of span concept

Closure characterization of a matroid

Definition: (E,c) is a matroid if $(\forall A \subseteq E)\ (\forall p, q \in E)$

$$p \notin c(A) \ \wedge \ p \in c(A \cup \{q\}) \Rightarrow q \in c(A \cup \{p\})$$

This property is called Steinitz Exchange Axiom.

Given rank r $\qquad$ c (X) = { x ⊂ E s.t r(X ∪ x) = r(X) }

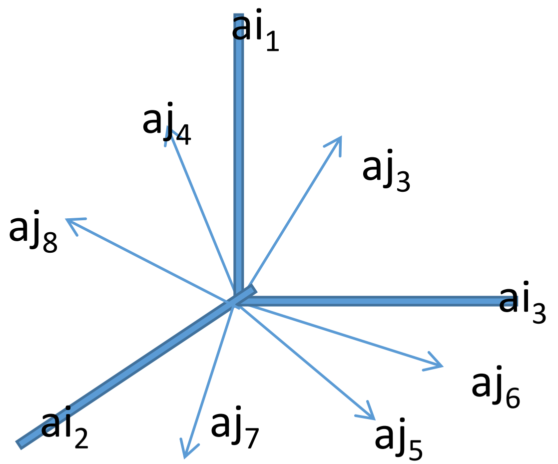
independent sets :

$$\boxed{I = \{ X \subset E \text{ s.t } X \subset c(X - x)\ \forall x \in X \}}$$

Span (X)= Span (ai_1, ai_2, ai_3) = R^3

Span (aj_1,aj_2,aj_3,aj_4,…aj_8)= R^3

Closure operator generalize the idea of span



Isomorphisms in between column vectors of matrices

LEMMA : For given $M_1, M_2 \in GF(2)^{r\times n}$

let a_i and b_i be their icolumn vectors

Assume $\exists \quad a_i \overset{\cong}{\to} b_i$,

Then $\exists$ matrix $A \in G(L_r)^2$ with

$$Aa_i = b_i \qquad \forall 1 \leq i \leq n$$

$$\underset{A}{\begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}} \times \begin{array}{c} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 7 \end{bmatrix} \\ \begin{array}{ccc} a_1 & a_2 & a_3 \end{array} \end{array} = \begin{array}{c} \begin{bmatrix} 8 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 21 \end{bmatrix} \\ \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \end{array}$$

$Colmat(M_1) \cong Colmat(M_2)$ if $rowspace(M_1) = rowspace(M_2)$.

Equivalence relation in between row subspaces of $GF(2)^n$

Definition: Two r-dimensional row subspaces $R_1 \sim R_2$ both in $GF(2)^n$).

if $\exists$ a permutation $\pi : \{1,\ldots,n\} \to \{1,\ldots,n\}$ s.t.

$$R_2 = \{(c_{\pi 1},\ldots,c_{\pi n}) \;|(c_1,\ldots,c_n) \in R_1\}$$

span($a_1\ a_2\ a_3\ a_4$) = $\begin{matrix} a_1 & a_2 & a_3 & a_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ a_3 & a_4 & a_1 & a_2 \end{matrix}$ = (1 3) (2 4) = span ($a_3\ a_4\ a_1\ a_2$)

$\Downarrow$

bijective equivalence relation between binary (n,r) codes

$\Updownarrow$

$b(n,r)$ isomorphic classes of binary rank r matroids on n elements.

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- ✓ Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Bounding the number of Isomorphic classes of binary r rank matroids on n elements (Asymptotic expression found by Wild)

$$\frac{1}{n!}\frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-r+1}-1)}{(2^r-1)(2^{r-1}-1)\dots(2^1-1)} \leq b(n,r) \leq \frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-r+1}-1)}{(2^r-1)(2^{r-1}-1)\dots(2^1-1)}$$

number of r-dimensional subspaces of $GF(2)^n$.

number of k-dimensional subspaces of an n-dimensional vector *space* $v(n,q)$ *is*

$$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(qk-1-1)\dots(q-1)} \; (k = 0, \dots, n)$$

the number $U_{n,k}$ *of* $k-tuples$ of linearly independent vectors in $V(n,q)$.

The Gaussian binomial coefficients and the bounds

The Gaussian binomial coefficients

$$\binom{m}{r}_q = \begin{cases} \frac{(1-q^m)(1-q^{m-1})\cdots(1-q^{m-r+1})}{(1-q)(1-q^2)\cdots(1-q^r)} & r \le m \\ 0 & r > m \end{cases}$$

m and *r* are non-negative integers.

For *r* = 0 the value is 1

Examples

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

$$\binom{1}{1}_q = \frac{1-q}{1-q} = 1$$

$$\binom{2}{1}_q = \frac{1-q^2}{1-q} = 1+q$$

$$\binom{3}{1}_q = \frac{1-q^3}{1-q} = 1+q+q^2$$

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

$$\binom{4}{2}_q = \frac{(1-q^4)(1-q^3)}{(1-q)(1-q^2)} = (1+q^2)(1+q+q^2) = 1+q+2q^2+q^3+q^4$$

K dimensional vector subspaces on a n dimensional vector space over F

the enumerative theory of projective spaces defined over a finite field. ⇨ Gaussian binomial coefficients

∀ finite field F_q with q elements, the Gaussian binomial coefficient $\binom{n}{k}_q$ counts the number $V_{n,k;q}$

different k-dimensional vector subspaces of an n-dimensional vector space over F_q (a Grassmanian).

example,

$$\binom{n}{1}_q = 1 + q + q^2 + \cdots + q^{n-1}$$

is the number of different lines in $F_q{}^n$ (a projective space)

The number of k dimensional subspaces from an n dimensional vector space **V(n,q)** is:

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)} \qquad (k = 0, \ldots, n).$$

Bounding the number of Isomorphic classes of binary r rank matroids on n elements

First coordinate of the tuple: v

take any one of the $q^n - 1$ vectors $v \neq 0$

Second Coordinate of the tuple : (v,w)

Since $v \neq 0$ spans a one dimensional subspace containing q vectors,

$q^n - q$ vectors linearly independent of v,

Third Coordinate of the Tuple:

v, w spans a two-dimensional subspace containing q^2 vectors,

$q^n - q^2$ linearly independent vectors of v, w,

$$U_{n,k} = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{k-1})$$

Each k-tuple of linearly independent vectors span a k-dimensional subspace

any k-dimensional subspace possesses $U_{k,k}$ ordered bases.

$$U_{k,k} = (q^k - 1)(q^k - q^2)\cdots(q^k - q^{k-1}).$$

$$\binom{n}{k}_q = \frac{U_{n,k}}{U_{k,k}},$$

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- ✓ Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Cauchy-Frobenius Counting theorem also called Burnside Lemma

Burnside Cauchy Frobenius Lemma

Lemma: (the orbit-counting theorem)

result useful in taking account of symmetry when counting mathematical objects.

Let G be a finite group that acts on a set X.

$g \in G$, let X_g denote the set of elements in X that are fixed by g.

States that $|\frac{X}{G}| = \frac{1}{|G|} \sum_{(g)inG} |X_g|$

number of orbits (a natural number or $+\infty$) = average number of points fixed by g G.

Transversal of orbits and the partition determined by a group action of a finite set.

Definition: The transversal of orbits

As G is an equivalence relation on X, a transversal F of the orbits yields a set partition of X, i.e, a complete dissection of X into the pairwise disjoint and nonempty subsets $G(t), t \in F$

$$X = \bigcup_{t \in F} G(t)$$

Hence the set of orbits will be denoted G

$$X := \{G(t) | t \in F\}$$

An Action of a group in a finite set equivalent to a permutation representation of the set.

Group Actions and Partitions

Each set partition of X gives rise to an action of a certain group on X.

let X_i ,where $i \in I$, an index set,

denote a partition of pairwise disjoint, nonempty sets which union is X.

An Action of G on a set X is equivalent to a permutation representation of G on X

it yields a set partition of X into orbits.

$$\bigoplus_i S_{x_i} := \{\pi \in S_x | \forall i \in I : \pi X_i = X_i\}$$

each set partition of X corresponds in a natural way to an action of

certain subgroup of the symmetric group S_x

which has blocks of the partition as its orbits.

Relationship fixed points and Stabilizers
(Frobenius-Cauchy- Polya)
Burnside Lemma

Stabilizers and Fixed points

orbits

$G(x) \subset$ X $\Longleftarrow$ $G_x \leq$ G

stabilizers.

X_g fix points

Stabilizer of $x \in X$ is $G_x := \{g | gx = x\}$

$x \in X$ is fixed under Fixed point g in G iff $gx = x$.

The set of all fixed points of G is $X_g := \{x | gx = x\}$

The set of all fixed points of a subset S in G is $X_S := \{g \in S | gx = x\}$
If $S = G$ we call it Set of invariants.

we say x is a fixed point of g and
g fixes x.

stabilizer subgroup of x (also called the isotropy)
is the set of all elements in G that fix x:

Natural bijection between Orbits and Cosets of Stabilizers

For a fixed x in X, consider map G to X

$$g \to g.x \text{ for all } g \in G.$$

image of this map is the orbit of x

the coimage is the set of all left cosets of G_x.

The standard quotient theorem of set theory

gives a natural bijection between G/G_x and Gx

given by $hG_x \to h.x$.

orbit-stabilizer theorem.

If G and X are finite then the orbit-stabilizer theorem, together with Lagrange's theorem, gives $|Gx| = [G : G_x] = |G|/|G_x|$.

This result can be employed for counting arguments.

The standard quotient bijection in between orbits and cosets of the Stabilizer

Standard Quotient Theorem:

The mapping $G(x) \to G/Gx : gx \to gG_x$ is a bijection ,

$gx = g'x \Leftrightarrow g^{-1}gx = g^{-1}g'x \Leftrightarrow x = g^{-1}g'x$

$\Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow G_x = g^{-1}g'G_x \Leftrightarrow g'G_x = gG_x$

$\Downarrow$

Corollary: If G is a finite group acting on set X , then $x \in X$

$$|G(x)| = |G|/|G_x|$$

Lagrange Theorem:

Lagrange's Theorem *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. number of distinct left cosets of H in G is $\frac{|G|}{|H|}$.*

$|G| = r|H|.$

$|a_iH| = |H|$ for each i,

$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$

cosets are disjoint,

$G = a_1H \cup \cdots \cup a_rH.$

a in G, $aH = a_iH$ for some i $a \in aH.$

$a_1H, a_2H, \ldots, a_rH$

distinct left cosets of H in G.

Orbit-Stabilizer Theorem

Corollary:

If G is a finite group acting on the set X , then for each $x \in X$

we have $|G(x)| = |G|/|G_x|$

$\Uparrow$

$G(x)$ has the same number of elements as G / G_x

$|G(x)| = [G : G_x]$

$\Uparrow$

$g * x \mapsto g\, G_x$

$\Uparrow$

there is a well-defined bijection:

$G(x) \to G / G_x$

$\Uparrow$

Standard Quotient Theorem

Proof Cauchy Frobenius Lemma

The number of orbits of a finite group G acting on a finite set X is equal to the average number of fixed points:

$$|G \backslash\backslash X| = 1/|G| \sum_{ginG} |X_g|$$

$$|G| \sum_{t \in F} (1) = |G|.|G \backslash\backslash X|$$

number of orbits of finite group G acting on a finite set X

$$\sum_{x \in G(t)} |G(x)|^{-1} = |G(x)||G(x)|^{-1} = 1$$

$$GX := \{G(t) | t \in F\}$$

F is transversal

$$\sum_x |G||G(x)|^{-1} = |G| \sum_x |G(x)|^{-1} = |G| \sum_{t \in F} \sum_{x \in G(t)} |G(x)|^{-1}$$

Orbit-Stabilizer Theorem

Enumerating elements in the Stabilizer

$$\sum_x \sum_{g \in G_x} 1 = \sum_x |G_x| =$$

Enumerating fixed points in G x X

$$\sum_{g \in G} |X_g| = |\{(g,x) \in G \times X | g.x = x\}| = \sum_{g \in G} \sum_{x \in X_g} 1$$

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- ✓ Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Number of orbits equals the average of fix points

The orbits of this group action correspond bijectively to the isomorphism classes of binary matroids of n elements with rank $\leq r$

Let $Z(A,\pi) := M \in Z : (A,\pi) * M = M$

Main Result : using Burnside lemma, the number of orbits is

$$b(n, \leq r) = \frac{\sum\limits_{(A,\pi) in GL_r^2 x S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

Here the number of orbits equals the average of fix points.

Also $b(n,r) = b(n, \leq r) - b(n, \leq r-1)$

Defining groups involved in the enumeration of the isomorphic classes of of binary r rank matroids on n elements

let us consider the group $GL_r^2 \times S_n$,

The group acts on the set $Z := GF(2)^{r\times n}$ of matrices $M := (a_1, a_2, ..., a_n)$

$$(A,\pi) * (a_1, ..., a_n) := (Aa_{p^{-1}1}, \ldots, Aa_{p^{-1}n})$$

Permutation group that change the order of the columns , moving columns with their Respective labels.

Non singular matrix
That represents a group which action is equivalent to all elementary row Operations (change of basis)

The general linear group of degree n through elementary matrices – the set

Set : n×n invertible matrices,

Operation: Ordinary matrix multiplication.

It is a group since:

- Product of two invertible matrices is again invertible,
- Inverse of an invertible matrix is invertible.
- Neutral element is the identity matrix.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2 \quad b_1c_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1} = \frac{1}{a_1d_1 - b_1c_1}\begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix} \qquad \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}^{-1} = \frac{1}{a_2d_2 - b_2c_2}\begin{bmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2 \quad b_1c_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}^{-1}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \qquad \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The elementary matrices generate the general linear group of invertible matrices.

Row switching

$$R_i \leftrightarrow R_j \qquad T_{i,j} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Row multiplication

$$kR_i \to R_i, \qquad k \neq 0 \qquad T_i(m) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & m & 0 & m & m \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Row addition

$$R_i + kR_j \to R_i, \; i \neq j \qquad T_{i,j}(m) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ m & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & m & 1 & m \end{bmatrix}$$

Left multiplication (pre-multiplication) by an elementary matrix represents elementary row operations,

Right multiplication (post-multiplication) represents elementary column operations.

Permutations notations and fixed points

Permutations:

Rearranging, members of a set into a particular sequence or order

Example,

Set {1,2,3}: (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), and (3,2,1).

The number of permutations of n distinct objects is n!

Cauchy's two-line notation:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};$$

Cycle notation: It expresses the permutation as a product of cycles corresponding to the orbits of the permutation

$$\sigma_1 = (1)(2)(3) \ ; \ \sigma_2 = (1)(2 \ \ 3) \ ; \ \sigma_3 = (1 \ \ 2)(3) \ ; \ \sigma_4 = (1 \ \ 2 \ \ 3) \ ; \ \sigma_5 = (1 \ \ 3)(2)$$

An orbit of size 1 is called a fixed point of the permutation.

The subgroup of all permutations for a given set

Symmetric group of S, Sym(S)

Set: all permutations of any given set S ,

Operation : Composition of maps (product)

Neutral element: Identity function .

Example,

(1,2,3), (1,2,3), (1,2,3), (1,2,3), (1,2,3), (1,2,3),

$\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$

(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1).

(1,2,3)

$\downarrow$

(1,3,2)

$\downarrow$

(3,2,1)

(1,2,3)

$\downarrow$

(3,2,1)

Left group action over a finite set

Left Group Action of Group G on Set X

Definition: a group G with binary operation($\bullet$)

function $G \times X \to X \quad s.t.$

$\forall g \in G$ and $x \in X$,

mapping $(g, x) \to g.x$ operation

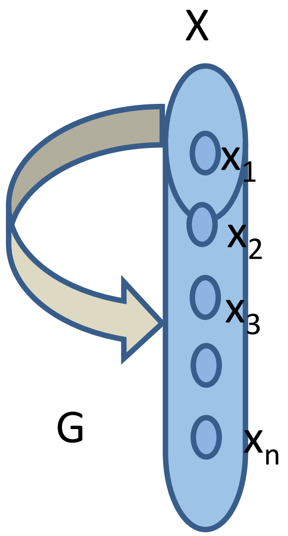
satisfies properties:

(i) compatibility $(g \bullet h).x = g.(h.x) \quad \forall g, h \in G \text{ and } \forall x \in X.$

(ii) identity $\exists\ e,\ s.t.\ \ e.x = x \quad \forall x \in X,$

e neutral element of G.

X is left $G - set.$



Right group action over a finite set

Right Group Action of Group G on Set X

Definition: a group G with binary operation$(\ast)$

function $X \times G \to X \quad s.t.$

$\forall g \in G$ and $x \in X$,

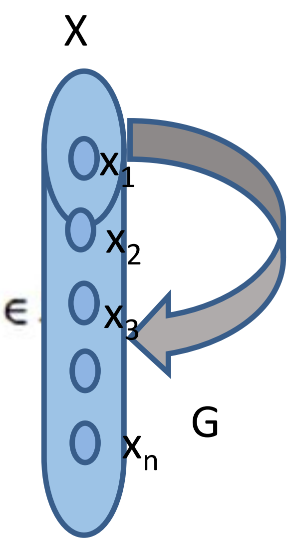
mapping $(x, g) \to x.g,$ operation

satisfying axioms:

(i) compatiblity: $x.(g.h) = (x.g).h = (x).g \ast h \quad \forall g, h \in G$ and $\forall x \in$

(ii) identity: $x.e = x \quad \forall x \in X$

X is right $G - set.$



Equivalence in between Left group action and Right group action on a finite set

left group action $\Leftrightarrow$ right group action

$$(g * h)^{-1} = h^{-1} * g^{-1}$$

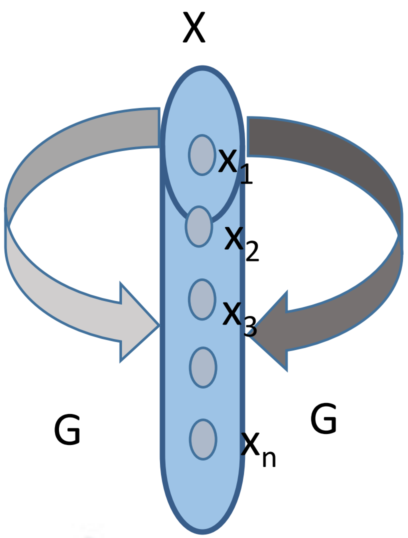
$$\forall g, h \in G \ and \ \forall x \in X.$$

left group action $(g*h).x =$

$$(g*h)^{-1}(g*h).x.(g*h)$$

$$(h^{-1} * g^{-1} g * h).x.(g*h) =$$

$$= x.(g*h)$$ right group action



Equivalence classes determined by the group action of G over X

Definition:

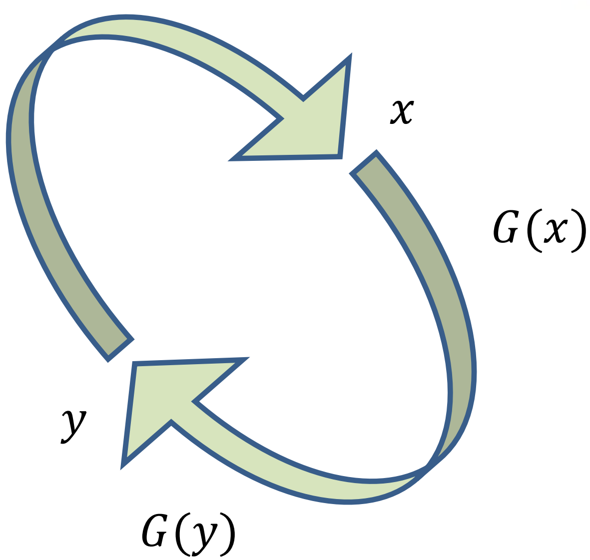
associated equivalence relationship $x \sim y$

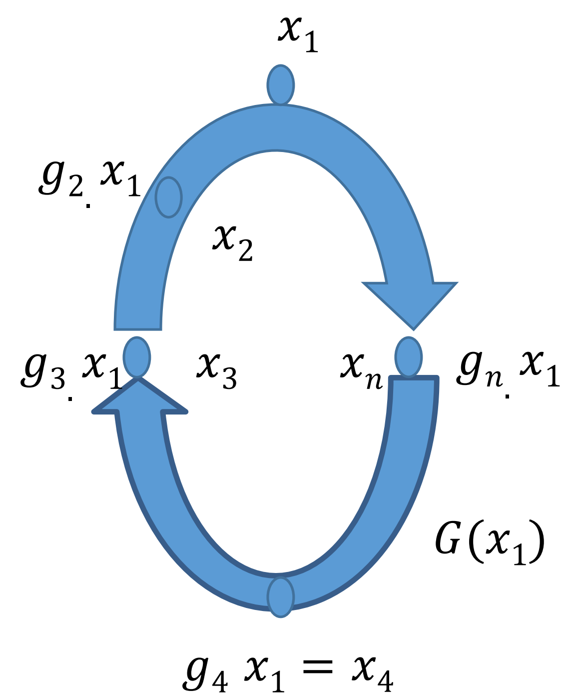
$$iff \quad \exists g \in G \;\; s.t, \;\; g.x = y \;.$$

We say that two elements x and y are equivalent

iff $Gx = Gy$.

The orbits are the equivalence classes .





Elements of G acting on an elements of a finite set X

Orbits in X under the action of the of group G.

The orbit of a point x in X is

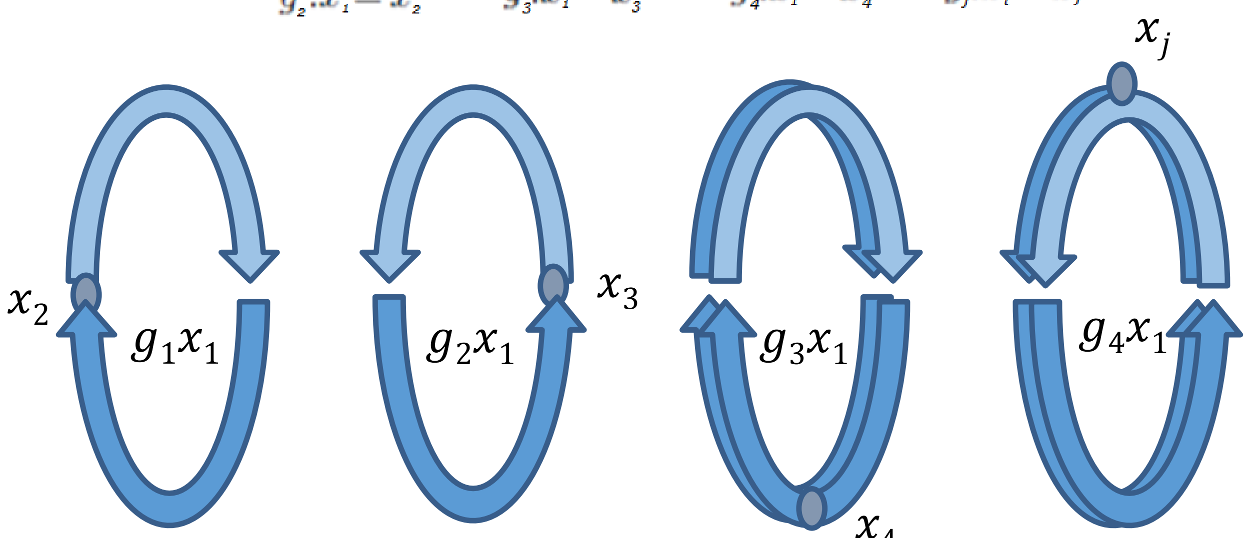
$$G.x := \{ g.x \mid g \in G \}$$

ORBITS AND PERMUTATIONS :

The orbit of x in X is the set of elements of X to which x can be moved by the elements of G.

$$G.x_i := \quad g.x_i = x_j$$

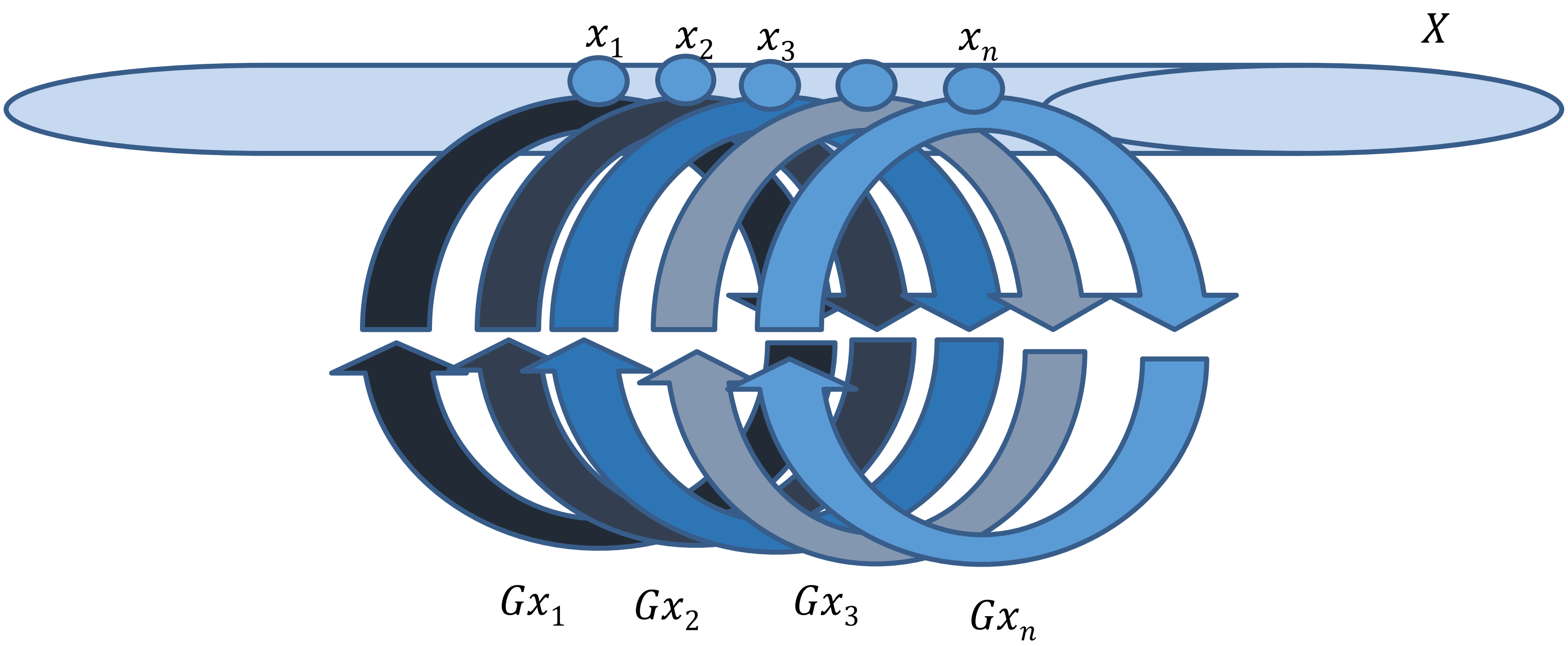
$g_2.x_1 = x_2$ $\quad g_3.x_1 = x_3$ $\quad g_4.x_1 = x_4$ $\quad g_j.x_i = x_j$



$$g_1x \; U \; g_2x \; U \; \dots U \; g_nx = G.x \text{ or } G(x)$$

A group acting on a finite set determines a partition on it.

The set of orbits of points $x \in X$, under action of G, form a partition of X.



The orbit space or quotient of the action of a group over a finite set

Orbit Space of the group action

Definition:

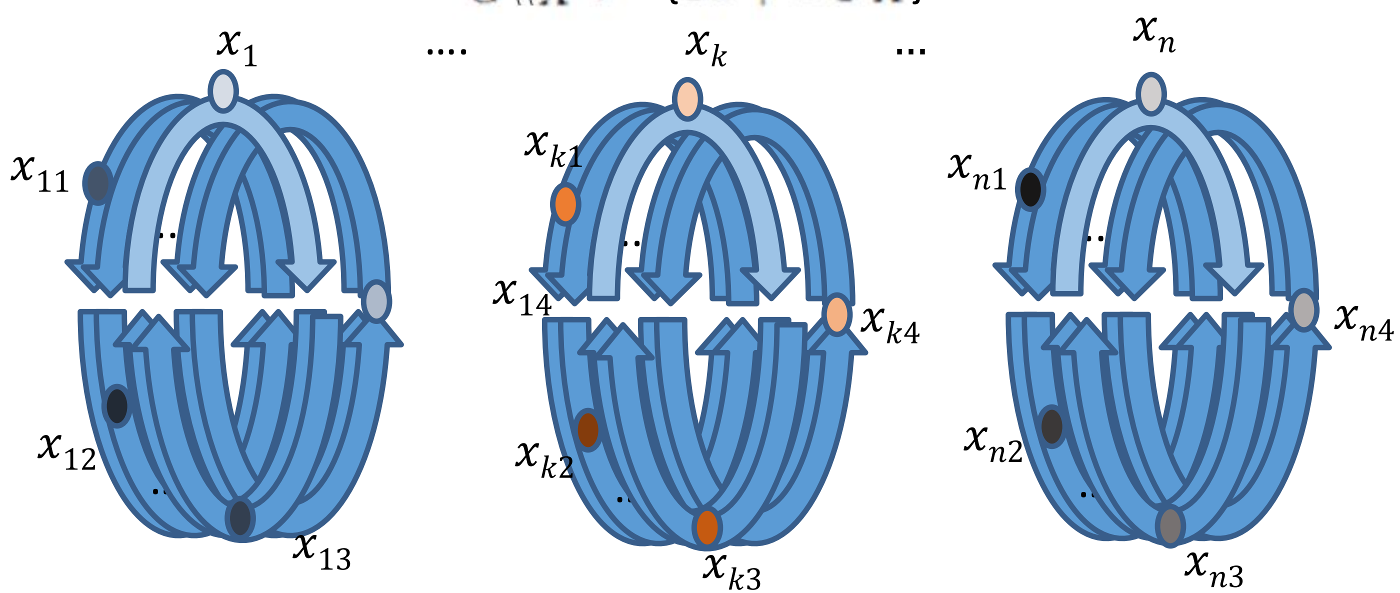
$$G\backslash X \quad G\backslash\backslash X \quad or \quad X//G \quad X/G$$

Orbit space or the quotient of the action

, the set of all orbits of X under the action G.

$$G\backslash\backslash X \quad \text{or} \quad G:X := \{\, g.x \mid g \in G \quad x \in X \,\}$$

$$G\backslash\backslash X := \{Gx \mid x \in X\}$$



$$Gx_1 \; U \ldots\ldots Gx_k \; U \quad \ldots . \, U \; Gx_n = G\backslash\backslash X$$

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- ✓ Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Reduction of the complexity of the counting operation by working with maps representation instead of matrix one.

difficulty to evaluate $|Z_{A,\pi}|$,

$\Downarrow$

so large number of summands.

$\Downarrow$

Burnside lemma can be refined

$\Downarrow$

instead of matrices $M \in GF(2)^{r\times n}$

$\Downarrow$

consider mappings

$$f : 1, 2, \ldots, n \to GF(2)^r.$$

$X := 1, 2, \ldots, n$ symmetric group action	$\Leftrightarrow$	$Y := GF(2)^r$ linear group action

act together

$$Y^X := f|f : X \in Y$$

$\Downarrow$

by the operation $(A, \pi) * f := Aofo\pi^{-1}$

Reduction of enumerating cost by using only one Composed Group Operator

Y_{A^i} ⇒ set of fix points ⇒ group element A^i $in\ GL_r^2$,

⇓

eigenspace of A^i of the eigenvalue $1 \in GF(2)$

$a_i(\pi)$ ⇒ number of cycles of length i

⇓

$\pi(1 \leq i \leq n)$ cycle decomposition

it is easy to compute Y_{A^i} $a_i(\pi)$

for a given

$A \in GL_r^2$, $\pi \in S_n$ and $1 \leq i \leq n$

Burnside lemma expression adapted to the rearrangement of the data in the Finite set and the Composed Group Operator already designed

the Burnside lemma can be refined as follows:

$$b(n, \leq r) = \frac{\sum_{(A,\pi) in GL_r^2 x S_n} \prod_{i=1}^{n} |Y_{Ai}|^{a_i(\pi)}}{|GL^2||S_n|}$$

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- ✓ Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Simplifying the averaging of fix points by using Conjugacy classes of representatives

Averaging the points on the matrices in Y fixed under the action of the linear group H^x
and
The points fixed on the row permutations of X under the action of the permutation symmetric subgroup G

through

the product of the fix points induced by canonical representatives of equivalences classes of elements of the two groups
determined
by
Conjugacy

with

The Cardinalities of the Sets of all such equivalence classes
in

groups G and in H

Burnside lemma expression readapted for conjugacy classes of matrices and permutations.

$$b(n, \leq r) = \frac{\sum\limits_{(A,\pi) in GL_r^2 x S_n} |Z_{A,\pi}|}{|GL^2||S_n|}$$

$$|H \wr_x G \backslash\backslash Y^x| = \frac{\sum\limits_{(\psi,g)\in H\wr_x G} \prod\limits_{v=1}^{c(g)} |Y_{h_v(\psi,g)}|}{|H^x||G|}$$

$$b(n, \leq r) = \frac{\sum\limits_{(A,\pi) in GL_r^2 x S_n} \prod\limits_{i=1}^{n} |Y_{A^i}|^{a_i(\pi)}}{|GL^2||S_n|}$$

$$b(n, \leq r) = \frac{\sum\limits_{\lambda\in Part(n) 1\leq\mu\leq k(r)} |C_\lambda||D_\mu| \prod\limits_{i=1}^{n} fix(\mu,i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Considering Conjugacy classes and number of points fixed by representatives of them.

Counting the points fixed on the matroids under the combined action of of both groups from the Wreath product by Considering the Conjugacy classes on the groups

$$b(n, \leq r) = \frac{\sum_{\lambda \in Part(n) 1 \leq \mu \leq k(r)} |C_\lambda||D_\mu| \prod_{i=1}^{n} fix(\mu,i)^{a_i(\lambda)}}{|GL_r^2||S_n|}$$

Notice here, that we have to count for each conjugacy class only the fixed points of only just one representative, since

by multiplying them by the cardinality of the sets of conjugacy classes of each of the groups involved in the wreath product we are in fact averaging all the fixed points of all the matroids that we are enumerating,

so by applying the burnside-Cauchy- Frobenius lemma in that way we are effectively enumerating nonisomorphic binary matroids

Conjugacy Classes of The Product of Two Groups

Theorem:

Let G and H be groups which have the sets of conjugacy classes C_G and C_H respectively. Then, if $C_{G \times H}$ denotes the set of conjugacy classes of $G \times H$ then

$$C_{G \times H} = \{\mathrm{A} \times B : A \in C_G \text{ and } B \in C_H\}$$

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathrm{GL}_n(\mathbf{F})$ to simplify computations.
- ✓ Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).
- Fix points of the conjugacy classes induced by $\mathrm{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

The Size of a conjugacy class in the symmetric group

Hence, the number of permutations in the conjugacy class described by the c_i 's is

$$|C_\lambda| = n!\left(\prod_{i=1}^{k} i^{c_i} \prod_{i=1}^{k} c_i!\right)^{-1}$$

The denominator is often called z_λ (for partitions of cycle type λ) when dealing with symmetric functions.

Counting the total number of Conjugacy Classes from the group of Permutations and their Partitions

define the conjugacy as follows:

$\pi\tau \in S_n$ are conjugate iff $a_i(\pi) = a_i(\tau)$ for all $1 \leq i \leq n$.

The conjugacy classes of S_n are in bijection with partitions of n,

sequences $\lambda = (\lambda_1, \ldots, \lambda_t)$ of natural numbers

satisfying

$$\lambda_1 + \ldots + \lambda_t = n \text{ and } \lambda_1 \geq \lambda_2 \geq \ldots \lambda_t.$$

λ is a partition of n $\qquad \lambda \vdash n$

The set of all partitions of n is:

$$Part(n) := \lambda | \lambda \vdash n$$

$\lambda_j = i$ is denoted as $a_i(\lambda)$

λ parametrize the conjugacy classes C_λ of the group S_n.

The Size of a conjugacy class in the symmetric group

Conjugation preserves cycle type,
Therefore by
specifying a cycle type,
That is equivalent to specify a partition of n,
we fully specify a
conjugacy class in S_n.

Decomposition of a Permutation to the direct sum of cyclic Permutations

Definition: (Type of a permutation)

let π be a permutation of the finite set S

$$|S| = d$$

$$\pi = \sigma_1 . \sigma_2 \cdots \sigma_n , \qquad \sigma_i \cap \sigma_j = \emptyset \ ,$$

$$S = S_1 \cup S_2 \cup S_n , \qquad S_i \subset S , \qquad \pi \, S_i = S_i$$

S_i is the minimal subset of S invariant under π.

The type of the permutation is $a(\pi) = (a_1(\pi), \ldots, a_d(\pi))$

where $a_i(\pi)$ is the number of cyles of length i in the cycle decomposition.

Introducing the Polya cycle Index

Definition: (Polya) cycle index)

let G is a permutation group on S,

the permutation cycle index,

also called Polya cycle index,

$$Z(G;x) = \frac{\sum_{\alpha \in G} \prod_{i,b} x_{i,b}^{a_{i,b(\alpha)}}}{|G|}$$

$Z(G;x)$ is the generating function of permutations in G,

Outline of Presentation

- Enumeration is possible since matrix representability is unique (Brilawky-Lucas theorem).
- Highest lower bound and Least upper bound of number of the isomorphic classes.
- Analytic enumeration of isomorphic classes through counting of orbit counting Theorem.
- Defining the suitable double group action required to apply the orbit counting Theorem.
- Rearranging the finite set in a format suitable for the ulterior simplification of the computation of the average of fix points.
- Averaging the fix points using conjugacy classes of S_n and $\mathsf{GL}_n(\mathbf{F})$ to simplify computations.
- Fix points of the conjugacy classes induced by S_n (Polya Permutations cycle index).

✓ Fix points of the conjugacy classes induced by $\mathsf{GL}_n(\mathbf{F})$ (Decomposition of linear Transformations & Canonical form Theory).

Conjugacy classes of the products of elementary matrices from the linear group that perform row operations for the change of basis

Conjugacy Classes of Products of Elementary matrices

elements of any group may be partitioned into conjugacy classes;

Let H^X be a group.

$$H^x = \{ \psi : (h_1. h_2, h_3, ... h_x) \mid h_i \in H\}$$

Two elements ψ and ψ' of H are conjugate if

$$\boxed{\psi_i \text{ in } H^X \text{ with } \psi_i \psi' \psi_i^{-1} = \psi}$$

conjugacy is an equivalence relation

partitions H^X into equivalence classes.

every ψ in H^X belongs to one conjugacy class

classes $Cl(\psi')$ and $Cl(\psi)$ are equal $\Longleftrightarrow$ ψ', ψ are conjugate, and disjoint otherwise.

the conjugacy class that contains

$$\boxed{Cl(\psi) = \psi_i \psi \psi_i^{-1} : \psi_i \in H^x}$$

Index of Common number of Fixed points in a Conjugacy class of products of Elementary Matrices,

Relationship among Fixed points vs Eigenvectors

D is the conjugacy class of matrices A in GL_r^2.

$D^i = A^i \mid A \in D$ are also a conjugacy classes.

$D_1, D_2, \ldots, D_{k(r)}$ are the conjugacy classes of GL_r^2

For all $1 \leq \mu \leq k(r)$ and all $1 \leq i \leq n$, we define

D_μ^i a similar classes of invertible matrices

$fix(\mu, i)$ be the common number of fixpoints of any matrix in D_μ^i,

$$Y = A^i Y$$

the number of eigenvectors (including zero) of any matrix A^i $(A \in D_\mu)$.

How many polynomials are needed to represent the Conjugacy class of Products of Elementary Matrices ?

set of conjugacy classes $D_1, D_2, \ldots, D_{k(r)}$ is naturally divided in to 2^{r-1} parts,

$$p(x) = x^r + c_{r-1}x^{r-1} + \ldots + c_1 x + 1 \quad (c_i \in GF(2)).$$

Suppose $p(x) = p_1(x)^{e_1} \ldots p_1(s)^{e_s}$ with $p_i(x)(1 \le i \le s)$

Let $(\epsilon 1, \ldots, \epsilon s)$ of number partitions $\epsilon_1 \vdash e_1 \ldots \epsilon_s \vdash e_s$

conjugacy class $D(p; \epsilon_1 \ldots, \epsilon_s)$

the number of conjugacy classes D_μ mapped from p(x) is

$$g(p(x)) = part(e_1) \ldots part(e_s).$$

p(x) has multiplicity 1, then $g(p(x)) = 1$,

$|g(p(x))| < 2$ since $1 \le \mu \le k(r) < 2^r$.

conjugacy classes D_μ of GL_r^2 are exhausted just processing

2^{r-1} polynomials p(x).

Cycle Structure of Linear Transformations over Finite fields

The main result of Kung

analogy in between cycle decomposition of a permutation

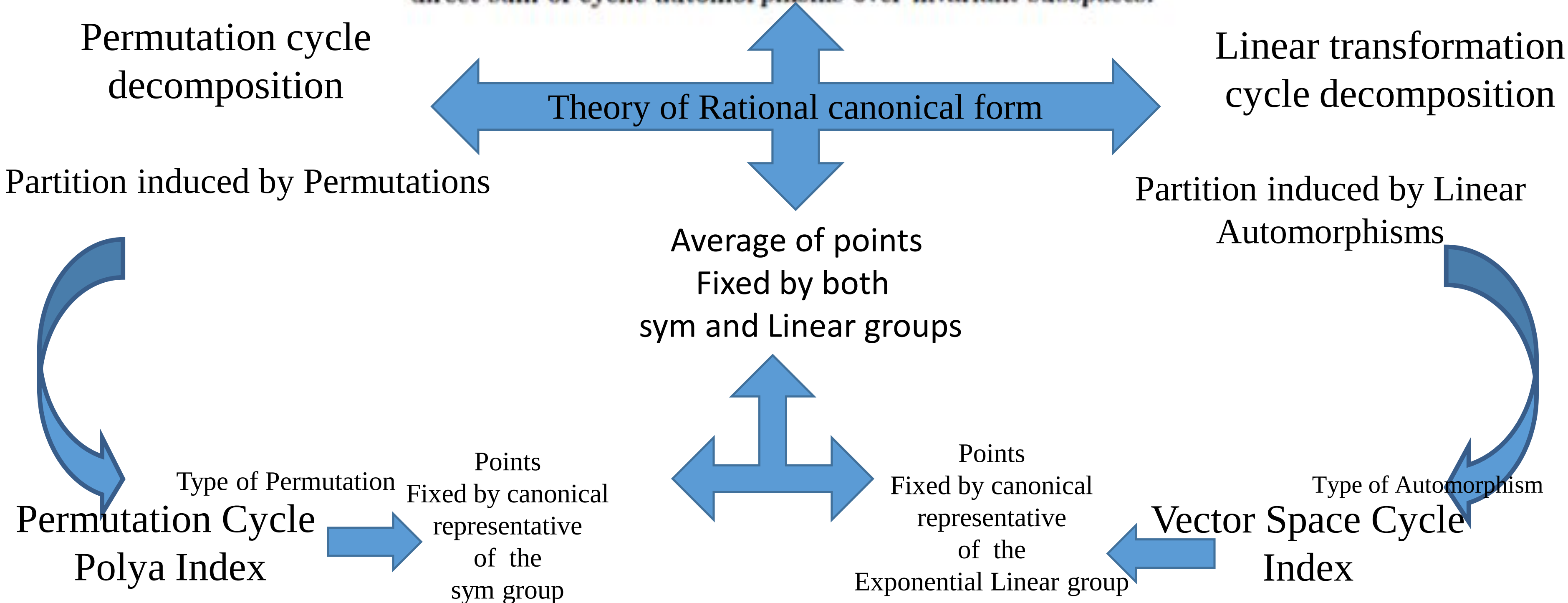
and

study of enumeration properties of the decomposition of an linear transformation

in to a diret sum of a cyclic linear transformations.

decomposition of an automorphism of a vector space in to a

direct sum of cyclic automorphisms over invariant subspaces.



Decomposition of an Automorphism in to the direct sum of cyclic automorphisms

Definition: (Vector space cycle index)

Let H be a finite linear group acting on the vector space V:

a finite subgroup of GL(V) of all automorphims of V.

Analogously to the Polya cycle index,

$x_{i,b}$, i positive integer

b a sequence of nonnegative integers

with finitely many nonzero terms.

The Vector space cycle index is given by:

$$Z(\mathrm{H}; x) = \frac{\sum\limits_{\alpha in G} \prod\limits_{i,b} |x_{i,bi}|^{a_{i,b}(\alpha)}}{|H|}.$$

, where $\prod\limits_{i,b} |x_{i,bi}|^{a_{i,b}(\alpha)}$ is

the weight of the automorphism.

The type of automorphism used to express number of points fixed
by a canonical automorphism in terms of the vector space cycle index.

Definition: (Type of the Automorphism α)

Let us associate with α an array $a(\alpha)$ its Type,
as follows:

Entries of $a(\alpha)$ are indexed by a pair (i, b),

i is a positive integer,

b is a sequence of nonnegative integers

with finitely many nonzero terms.

$a_{i,b}(\alpha)$ is the number of subspaces U

in the primary decomposition of α of order $p(z)^i$,

$p(z)$ is irreducible of degree i,

α restricted to U having species b.

The array $A(\alpha)$ has finitely

many nonzero entries.

$$a(\alpha) = \begin{pmatrix} a_{i,b}(\alpha) \cdots & a_{i,b}(\alpha) & a_{i,b}(\alpha) \\ \vdots \quad \cdots & \vdots & \vdots \\ \quad \cdots & & \\ a_{i,b}(\alpha) \ldots & a_{i,b}(\alpha) & a_{i,b}(\alpha) \end{pmatrix}$$