Construction of isomorphic classes of linear Binary codes

Based on Reseach By Harald Fripertinger, Adalbert Kerber and Reinhard Laue,

Presentation by:
Alexander Erick Trofimoff
PhD program
ECE Dept
Drexel U
2015 Winter

Bibliography

Betten A., Braun M., Fripertinger H., Kerber A., Kohnert A.,, Wasserman A., Error Correcting Linear Codes – Classification by Isometry and Applications , Springer Algorithmics and Computations in Mathematics Vol 18, 2006

Presentation Outline

- ✓ **Representing Graphically the Orbits**
- The orbit Data Structure
- Enumerating points of projective vector spaces using ranks
- Lexicographic ordering
- Arranging points of projective spaces in a order trees
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- Constructing all (n,k, q, dmin≥ 3) using Orderly Generation of codes (canonical subsets can be computed

Computing with permutation Groups

Action Graph :

Let a group G acting on a finite set X

Assume G is generated by a set of generators S={s_0,…,s_{r-1}}

The action group of G on X w.r.t set S is the

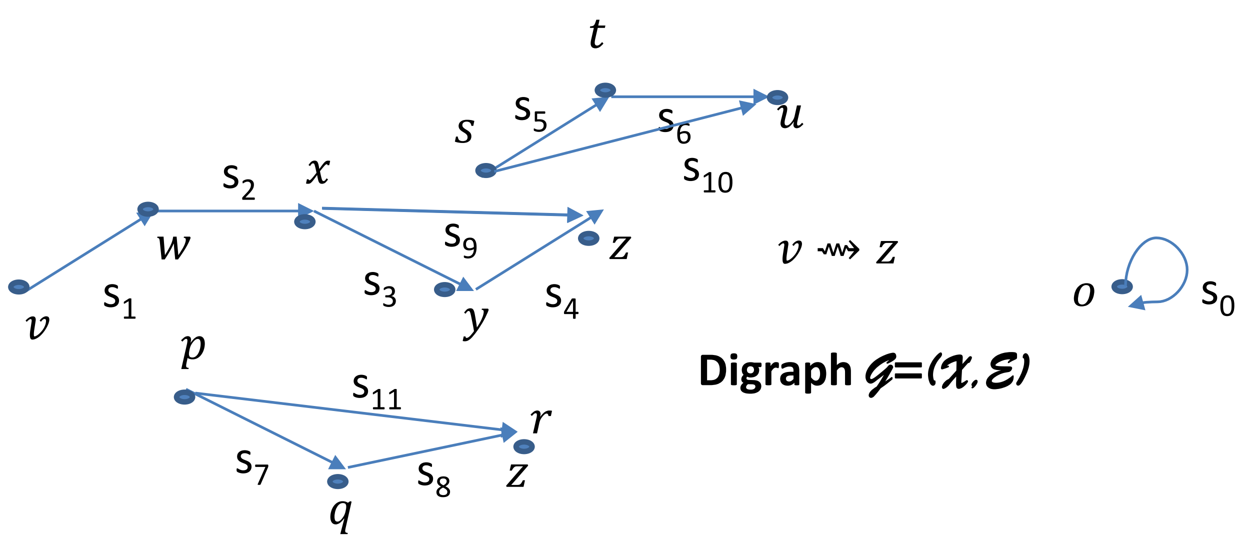
Digraph $\mathcal{G}=(\mathcal{X},\mathcal{E})$

$\mathcal{X}$: set of vertices

$\mathcal{E}$: set of edges

Let x and y be vertices and s_j be the edge that join them

$x\,s_j = y$. Now if there is a path from x to y we write $x \rightsquigarrow y$



Digraph $\mathcal{G}=(\mathcal{X},\mathcal{E})$

Computing with permutation Groups

Lemma

Let the group G act on a finite set X

Let $\mathcal{G}=(\mathcal{X},\mathcal{E})$ be the action graph w.r.t the generating

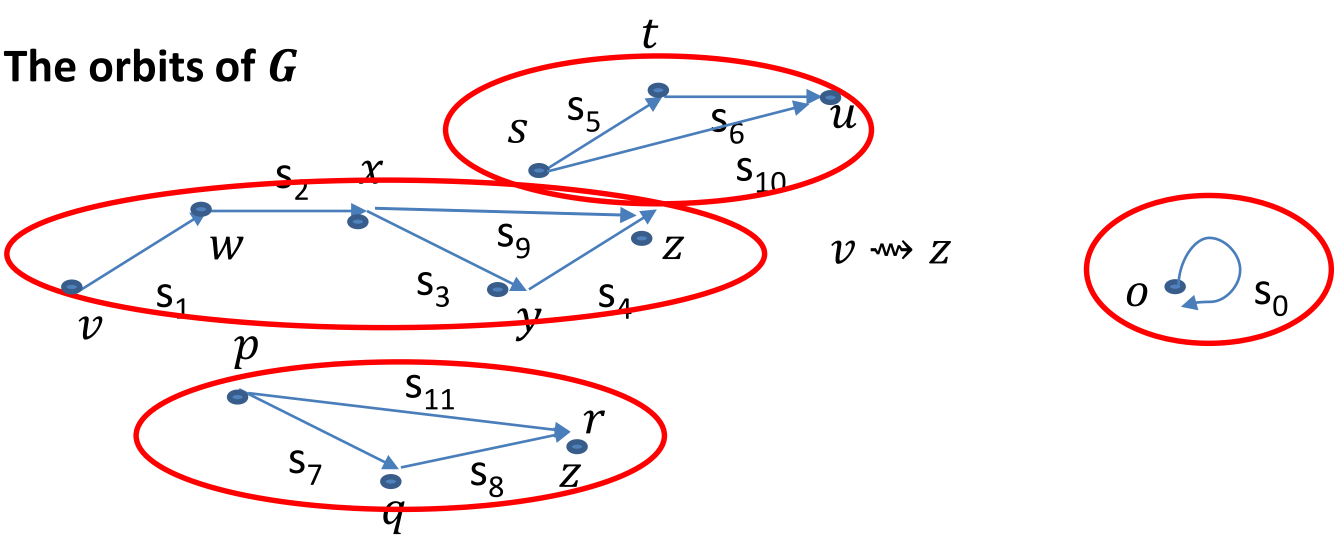
Set S of G.

Then, the orbits of G corresponds one to one with the connected Components of G. The components of G are well defined and independent of the choice of the generating set S of G .

Remark: A subset set U of vertices in a digraph is called strongly connected if both

$x \rightsquigarrow y$ and $y \rightsquigarrow x\ hold\ \forall \in U$

The orbits of G



Example

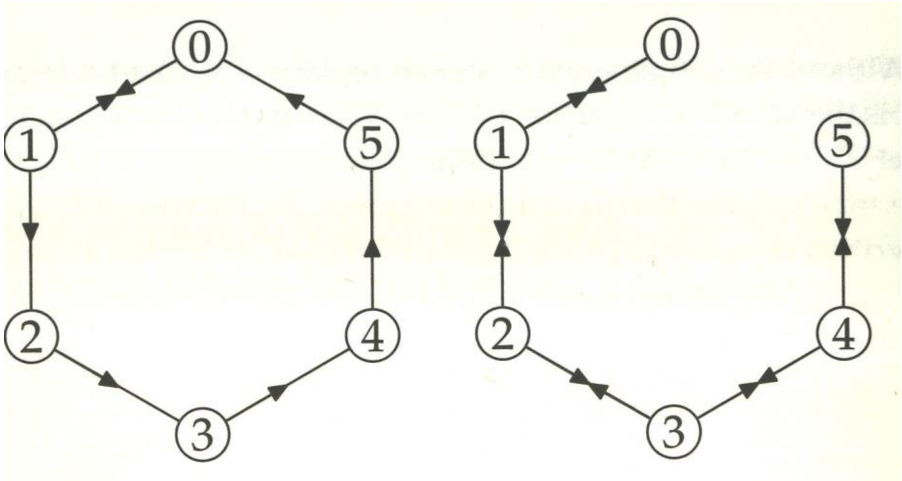


Fig. 9.1 Two action-graphs for S_6

Generated by

s_0 =(0,1,2,3,4,5)

s_i=(i,i+1)

s_1=(0,1)

Schreier Tree

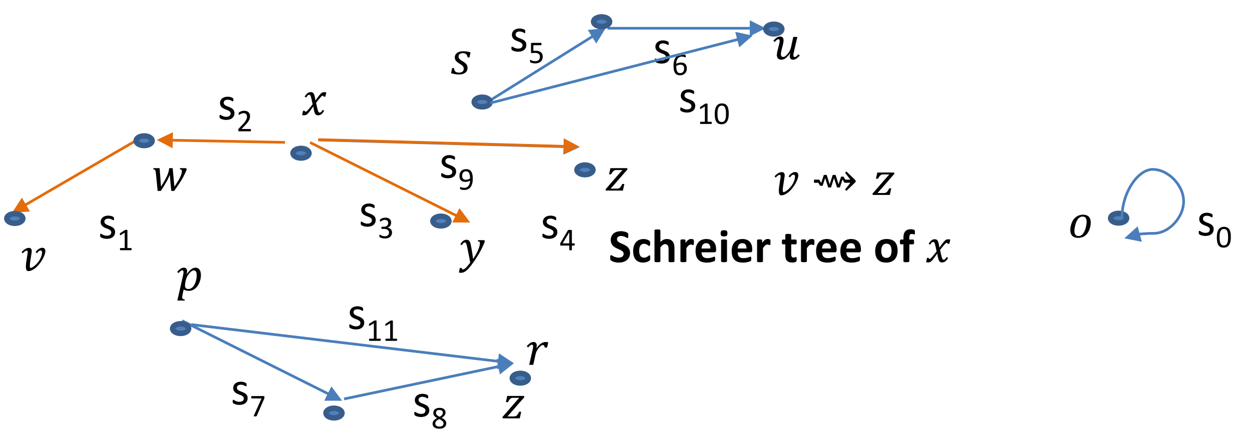
Let the group G act on a finite set X

Let G given by generators from s_0 to s_{r-1}

Let $\mathcal{G}=(\mathcal{X},\mathcal{E})$ be the action graph for G acting on X.

Let $x \in X$.

A Schreier Tree for the orbit of x is the spanning tree for the connected Component of G containing x.

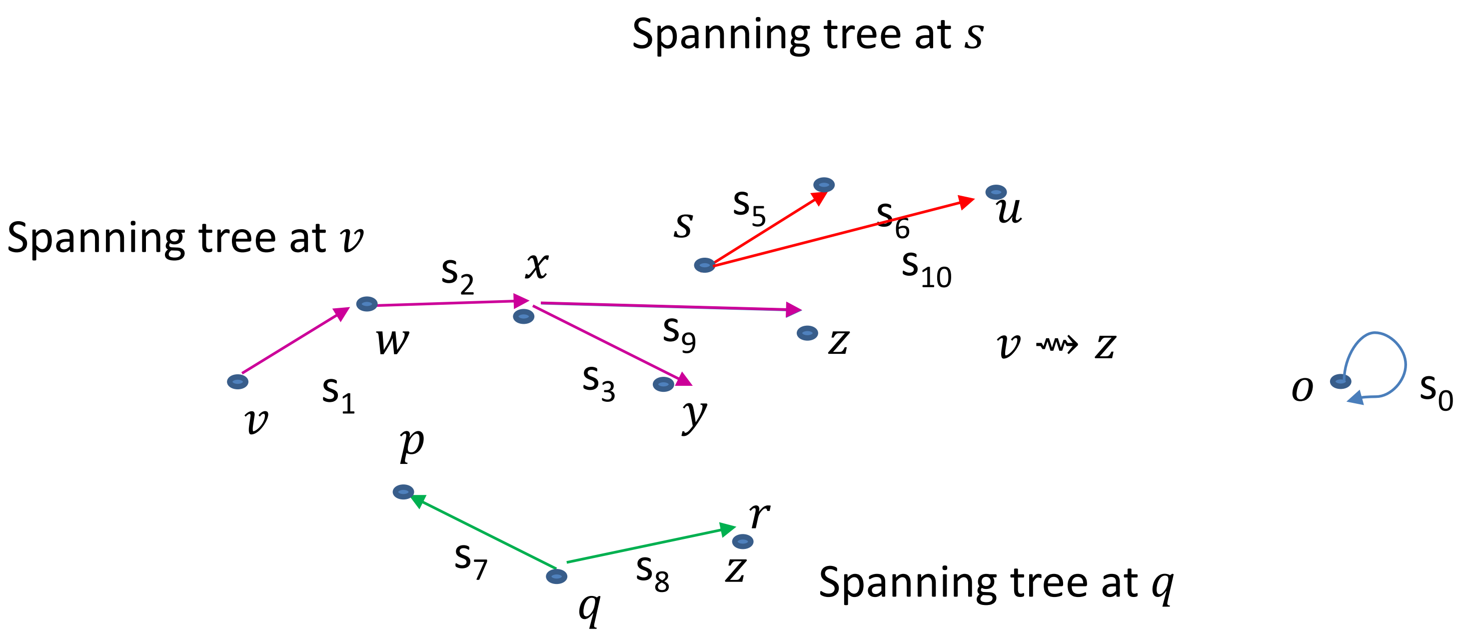


Schreier tree of x

Computing with permutation Groups

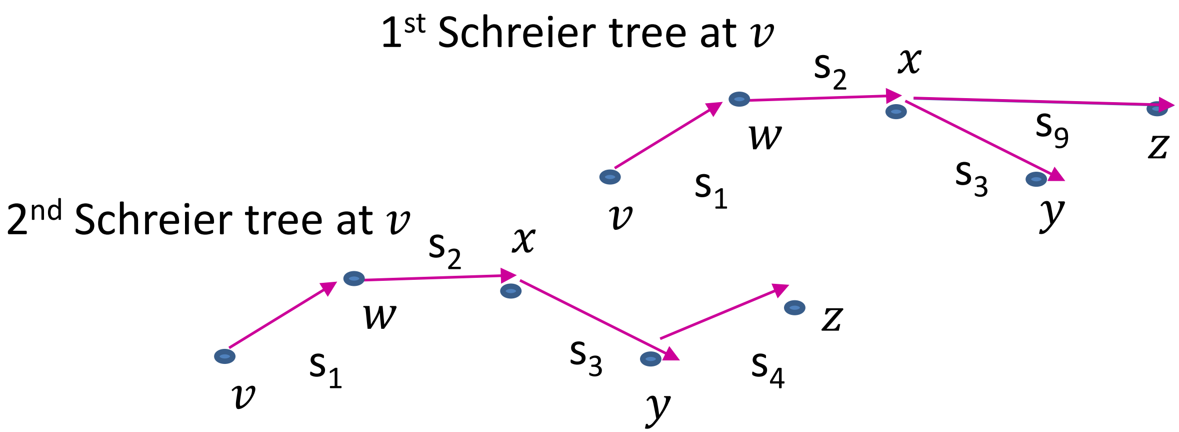
Schreier Tree

Remark: The tree is rooted at the respective *element*
and
all edges are pointed away from it.



Schreier Tree

The spanning tree for a connected component of a graph is not unique.
Since we can get $g_1.\,v = y = g_2.\,v$
for $g_1, g_2 \in G$



Algorithm (orbits on points)

Input: A permutation group G acting on a finite set $X = \{x1, . .$
$. , xn\}$, a
generating set $S = \{s0, . . . , sr-1\}$ of G, a point $x \in X$.

Output: A Schreier-tree $T = (O, E)$ for the orbit $O = G(x)$.

(1) let Q be a queue holding the element x

(2) let $O := \{x\}$, $E = \emptyset$, so that $T = (\{x\},\emptyset)$ has only one node x

(3) **while** $Q = \emptyset$ **do**

(4) let y be the first element of Q (remove y from Q)

(5) **for** $i \in r$ **do**

(6) $z := ysi$

(7) **if** $z \in O$ **then**

(8) append z to Q, add z to O

(9) add the edge (y, z) labeled by si to E

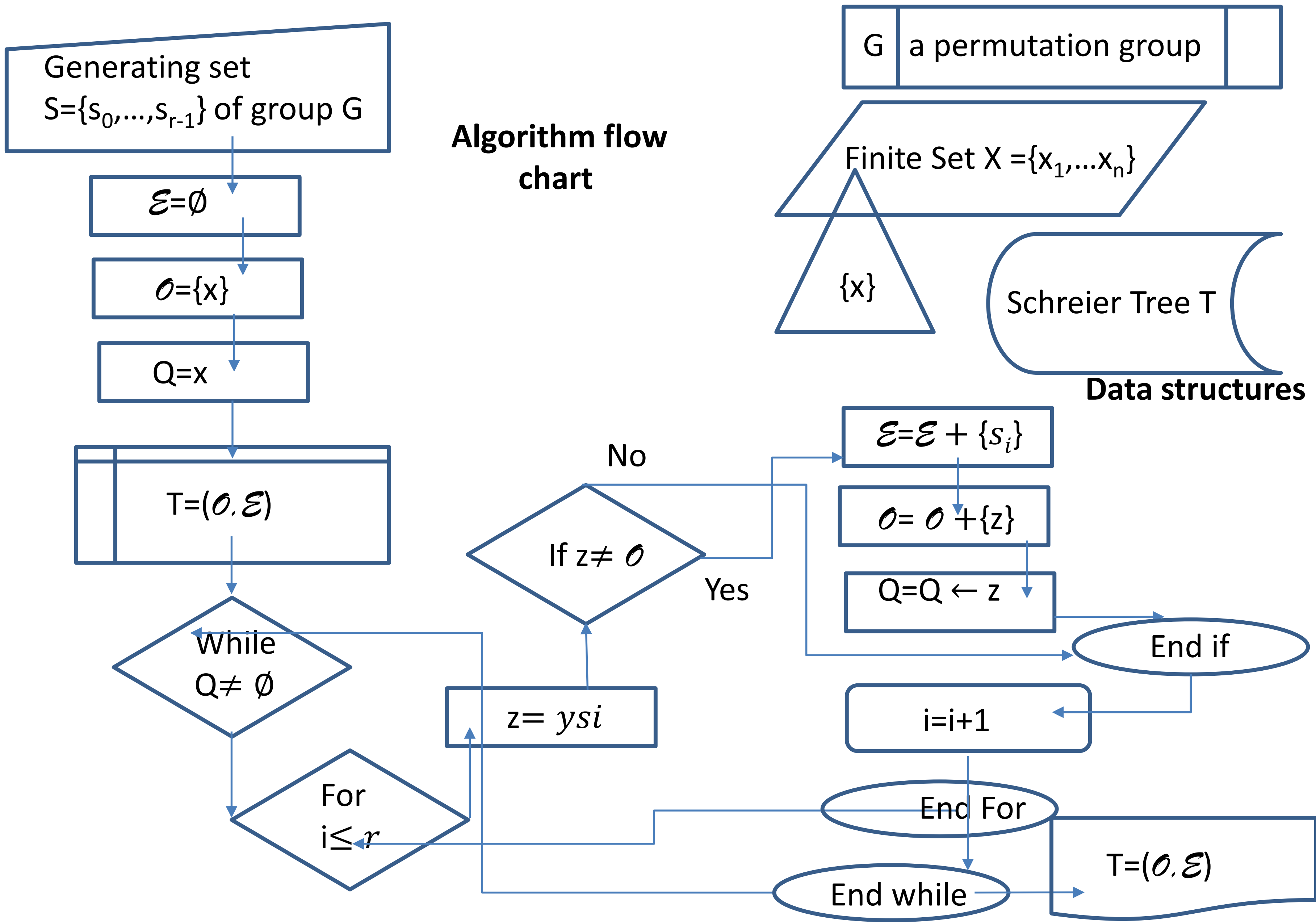
(10) **end if**

(11) **end for**

(12) **end while**

Here queue is a data structure similar than a waiting line, so the front most
Element is processed first and so for until all elements and the queue become empty.

Compute Orbits subroutine



Example

Example Let G be the permutation group generated by

$$\begin{aligned}
s_0 &= (3,4)(9,14)(10,13)(11,12), \\
s_1 &= (3,9)(4,14)(10,11)(12,13), \\
s_2 &= (3,11)(4,12)(9,10)(13,14), \\
s_3 &= (2,3)(6,9)(7,10)(8,11), \\
s_4 &= (1,2)(5,6)(10,12)(11,13), \\
s_5 &= (0,1)(6,7)(9,10)(13,14).
\end{aligned}$$

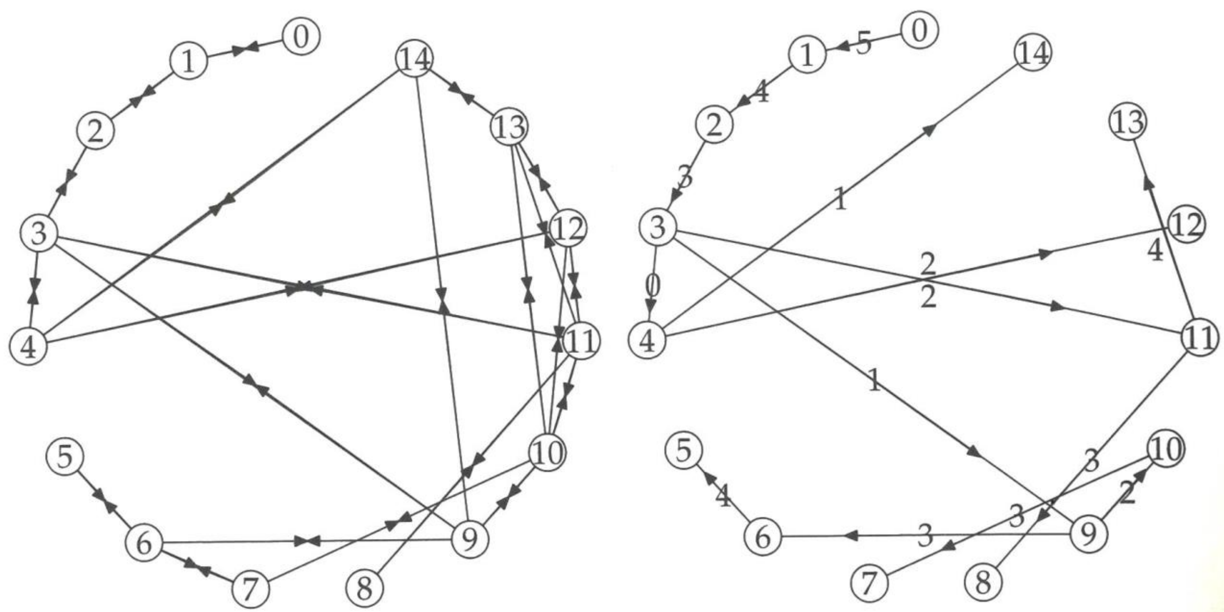


Fig. 9.2 Action-graph and Schreier-tree

Presentation Outline

- Representing Graphically the Orbits
- ✓ **The orbit Data Structure**
- Enumerating points of projective vector spaces using ranks
- Lexicographic ordering
- Arranging points of projective spaces in a order trees
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- Constructing all (n,k, q, dmin≥ 3) using Orderly Generation of codes (canonical subsets can be computed

Orbit data Structure

Let G be a group which acts on a finite set X

Orbit (G, X)=(τ, σ, φ) := (τ, σ, φ)

Is the **orbit data for G** acting on X provided that

1. τ is a transversal of the G -orbits on X
2. $\sigma: X \to L(G)$: $x \mapsto G_x$
3. φ: $X \to G$: $x \mapsto g$ with $xg \in \tau$

$L(G)$is the lattice of subgroups of G , $L(G)$={U| U≤ G}

σ: stabilizer map

φ: transporter map

G_x= {s ∈ G | sx = x } **Stabilizer**

For x,y ∈ X , y∈ $G(x)$, ∃g ∈ G *: xg=y , g is the* ***Transporter element***

Presentation Outline

- Representing Graphically the Orbits
- The orbit Data Structure
- ✓ **Enumerating points of projective vector spaces using ranks**
- Lexicographic ordering
- Arranging points of projective spaces in a order trees
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- Constructing all (n,k, q, dmin$\geq$ 3) using Orderly Generation of codes (canonical subsets can be computed

Permutation representation

Enumerating the points of finite projective spaces

Ass. $\kappa_{0,}\ \kappa_1, \kappa_2, \kappa_3, \ldots,\ \kappa_{q\text{-}1}$ be elements of the field F_q

With κ_0 =0 and κ_1 =1

We want to rank points of $\mathrm{F}_q{}^k$ $=\{\sum_{i=0}^{k-1} v_i e^{(i)} \mid v_i \in \mathrm{F}_q\}$

s.t. for any integer m=$(a_{k-1}, \ldots . a_0)_q$, $\mathrm{m}=\sum_{i\in k} a_i q^i$

Lemma

Let q be a prime power , m∈ q^k , with $\mathrm{m}=(a_{k-1}, \ldots . a_0)_q$

The map

$$rk_{k,q}{}^{-1}: q^k \to \mathrm{F}_q{}^k: \ ,\ \mathrm{m} \mapsto (\kappa_{a_0}, \ldots, \kappa_{a_{k-1}})$$

is a bijection that is called the unrank function for $\mathrm{F}_q{}^k$.

Its inverse $rk_{k,q}: \mathrm{F}_q{}^k \to q^k : (\kappa_{a_0}, \ldots, \kappa_{a_{k-1}}) \mapsto \mathrm{m}$ is the rank function.

Rank function & Unrank function in the Euclidean space

Example:

$rk_{2,3}$((0,0))=0 ; $rk_{2,3}$((1,0))=$rk_{2,3}$($e^{(0)}$)= 1; $rk_{2,3}$((2,0))= 2;
$rk_{2,3}$((0,1))=$rk_{2,3}$($e^{(1)}$)= 3 ; $rk_{2,3}$((1,1))=4; $rk_{2,3}$((2,1))=5;
$rk_{2,3}$((0,2))=6; $rk_{2,3}$((1,2))=7; $rk_{2,3}$((2,2))=8 ,

$rk_{2,3}^{-1}$(0)=(0,0) ; $rk_{2,3}^{-1}$(1)=($e^{(0)}$)= (1,0); $rk_{2,3}^{-1}$(2)= (2,0);
$rk_{2,3}^{-1}$(3)=($e^{(1)}$)=(0,1) ; $rk_{2,3}^{-1}$(4)=(1,1); $rk_{2,3}^{-1}$(5)=(2,1);
$rk_{2,3}^{-1}$(6)=(0,2); $rk_{2,3}^{-1}$(7)=(1,2); $rk_{2,3}^{-1}$(8)=(2,2) ,

Rank function & Unrank function Used to order vectors in the Projective space $\mathrm{PG}_d(q)$

- ✓ This is a typical sorting problem over a set of vectors using rank functions.
- ✓ The idea is to map the set of Projective spaces into a list of ranks, then we sort them and once they are already enumerated the unrank function is used to map backward. This provides a enumerated list of Projective spaces.
- ✓ For the Euclidean space, it is solved applying one only criteria.
- ✓ For the Projective space, it is solved using an additional second sorting criteria.
- ✓ The idea is to achieve is to sort based on the index of the right most non zero element, then sort based on the Euclidean space rank for representatives with the same index for the right most non zero element.

Rank function & Unrank function Used to order vectors in the Projective space $\mathrm{PG}_d(q)$

Let us enumerate set of 1-dim subspaces $\langle v \rangle$ of $\mathrm{F}_q{}^{d+1}$ $\quad v \neq 0$

$$|PG_d(q)| = \frac{q^{d+1}-1}{q-1} = q^d + q^{d-1} + \dots + q + 1 = \theta_d(q)$$

If $u \in PG_d(q) \quad \Rightarrow \quad u = \langle u_0 e^{(0)} + u_1 e^{(1)} + \cdots + u_d e^{(d)} \rangle \in PG_d(q)$

To enumerate 1-dim spaces we pickup representatives

$u = (u_0, u_1, \dots, u_d) \in \mathrm{F}_q{}^{d+1}$, whose rightmost coordinate is 1 .

$u_k = 1$; $u_{k+1, \dots,} u_d = 0$

$rk\,(e^{(0)}) = 0$; $rk\,(e^{(1)}) = 1$;… $rk\,(e^{(d)}) = d$; this in order to form a base

$rk\,(e^{(0)} + e^{(1)} + \dots + e^{(d)}) = d+1$

$u = (u_0, u_1, \dots, u_{k-1}, 1, 0, 0, \dots, 0)$ remaining vectors

With $(u_0, u_1, \dots, u_{k-1}) \in F_k(q) \backslash \{0\}$, $k = \mathrm{lc}(u)$

If $k = d$ then $(u_0, u_1, \dots, u_{k-1}) \neq (1, \dots, 1)$

Rank function & Unrank function Used to order vectors in the Projective space $PG_d(q)$

We decide to order these vectors:

1st according with the value of k , (from 1 to d).

2nd among the values of u for a given k, we order according with ranks of $(u_{0,} u_{1, \dots,} u_{k-1})$,

That is, $rk_{k,q} : F_q{}^k \to q^k : (\kappa_{a_0}, \dots, \kappa_{a_{k-1}}) \mapsto$ m

3rd we skip the 0 vector, since can't occur.

4th if If k= d then we skip (1,…,1)

5th (1,…,1) has rank $= \frac{q^d - 1}{q-1}$ = q^{d-1} +…..+ q + 1 = $\theta_{d-1}(q)$

6th increase all ranks which are greater than or equal to this number by 1 .

7th Shift the rank before to apply $rk_{k,q}{}^{-1}: q^k \to F_q{}^k:$, m $\mapsto (\kappa_{a_0}, \dots, \kappa_{a_{k-1}})$

8th if we are ranking u with lc(u) = d, decrease all ranks of $(u_{0,} u_{1, \dots,} u_{d-1})$, $\in F_q{}^d$ by 1 if they happen to be greater than $\theta_{d-1}(q)$.

9th Shift the rank before apply $rk_{k,q} : F_q{}^k \to q^k : (\kappa_{a_0}, \dots, \kappa_{a_{k-1}}) \mapsto$ m

Ordering procedure of a set X using rank functions.

1. We choose non zero representatives of each projective space.
2. Decompose the representatives using the standard basis so that we have vectors of coefficients.
3. We fix the unit vectors, as well as the all 1's vector , to occupy the first d places in the enumeration.
4. With the right most non zero element as the kth element, the rank is k.
5. Shift based on $\theta_{d-1}(q)$ so that all the vectors with higher ranks are increased by 1.
6. And representatives with the same k index for the right most non zero element are ordered based on the Euclidean space rank of the first k-1 elements.

$$\mathrm{rk}^{-1}_{d;q} : \theta_d(q) \to \mathrm{PG}_d(q) \qquad \mathrm{rk}_{d;q} : \mathrm{PG}_d(q) \to \theta_d(q)$$

Rank function & Unrank function in the Projective space $\mathrm{PG}_d(q)$

$$rk_{k,q}^{-1}(m) = \begin{cases} \langle e^{(m)} \rangle & \text{if } m \le d \\ \sum_{i=0}^{d} e^{(i)} & \text{if } m = d+1 \\ \langle rk_{k,q,d}^{-1}(m-d-1) \rangle & \text{otherwise} \end{cases}$$

where

$$\mathrm{rk}^{-1}_{d,k;q}(m) = \begin{cases} \mathrm{rk}^{-1}_{d,*;q}(m) & \text{if } k = d \\ e^{(k)} + \mathrm{rk}^{-1}_{k,q}(m) & \text{if } m < q^k \\ \mathrm{rk}^{-1}_{d,k+1;q}(m - q^k + 1) & \text{otherwise.} \end{cases}$$

Here,

$$\mathrm{rk}^{-1}_{d,*;q}(m) = e^{(d)} + \mathrm{rk}^{-1}_{d,q}(\mathrm{shift}_{\theta_{d-1}(q)}(m))$$

with

$$\mathrm{shift}_j(m) := \begin{cases} m & \text{if } m < j, \\ m+1 & \text{otherwise.} \end{cases}$$

This map $\mathrm{rk}^{-1}_{d;q}$ *is a bijection. Its inverse is the* rank function *for* $\mathrm{PG}_d(q)$*, denoted as* $\mathrm{rk}_{d;q}$. *For a point* $\langle u \rangle$ *with* $u = (u_0, u_1, \ldots, u_d) \in \mathbb{F}_q^{d+1} \setminus \{0\}$ *one has* $\mathrm{rk}_{d;q}(\langle u \rangle) =$

$$\begin{cases} k & \text{if } \langle u \rangle = \langle e^{(k)} \rangle \\ d+1 & \text{if } \langle u \rangle = \langle 1, \ldots, 1 \rangle \\ d + 2 - k + q\theta_{k-2}(q) + \mathrm{rk}_{k,q}\left(\frac{u_0}{u_k}, \ldots, \frac{u_{k-1}}{u_k}\right) & \text{if } k = \mathrm{lc}(u) < d \\ 2 + q\theta_{d-2}(q) + \mathrm{shift}^{-1}_{\theta_{d-1}(q)}\left(\mathrm{rk}_{d,q}\left(\frac{u_0}{u_d}, \ldots, \frac{u_{d-1}}{u_d}\right)\right) & \text{if } \mathrm{lc}(u) = d. \end{cases}$$

Example of how to enumerate using the rank functions

Example We have $\theta_2(2) = 2^2+2+1 = 7$, $\theta_2(3) = 3^2+3+1 = 13$ and $\theta_3(2) = 2^3+2^2+2+1 = 15$. Table shows the labeling of points of $PG_2(2)$, $PG_2(3)$ and $PG_3(2)$.

$$\begin{aligned}
\mathrm{rk}^{-1}_{3;2}(4) &= \langle 1,1,1,1\rangle \\
\mathrm{rk}^{-1}_{3;2}(5) &= \langle \mathrm{rk}^{-1}_{3,1;2}(1)\rangle \\
&= \langle e^{(1)} + \mathrm{rk}^{-1}_{1,2}(1)\rangle \\
&= \langle e^{(1)} + e^{(0)}\rangle = \langle 1,1,0,0\rangle \\
\mathrm{rk}^{-1}_{3;2}(14) &= \langle \mathrm{rk}^{-1}_{3,1;2}(10)\rangle \\
&= \langle \mathrm{rk}^{-1}_{3,2;2}(9)\rangle \\
&= \langle \mathrm{rk}^{-1}_{3,3;2}(6)\rangle \\
&= \langle \mathrm{rk}^{-1}_{3,*;2}(6)\rangle \\
&= \langle e^{(3)} + \mathrm{rk}^{-1}_{3;2}(\mathrm{shift}_7(6))\rangle \\
&= \langle e^{(3)} + \mathrm{rk}^{-1}_{3;2}(6)\rangle \\
&= \langle e^{(3)} + e^{(2)} + e^{(1)}\rangle = \langle 0,1,1,1\rangle \\
\mathrm{rk}^{-1}_{2;3}(12) &= \langle \mathrm{rk}^{-1}_{2,1;3}(9)\rangle \\
&= \langle \mathrm{rk}^{-1}_{2,2;3}(7)\rangle \\
&= \langle \mathrm{rk}^{-1}_{2,*;3}(7)\rangle \\
&= \langle e^{(2)} + \mathrm{rk}^{-1}_{2;3}(\mathrm{shift}_4(7))\rangle \\
&= \langle e^{(2)} + \mathrm{rk}^{-1}_{2;3}(8)\rangle \\
&= \langle e^{(2)} + 2e^{(1)} + 2e^{(0)}\rangle = \langle 2,2,1\rangle
\end{aligned}$$

$$\mathrm{rk}^{-1}_{d;q}(m) = \begin{cases} \langle e^{(m)}\rangle & \text{if } m \le d, \\ \langle \sum_{i=0}^{d} e^{(i)}\rangle & \text{if } m = d+1, \\ \langle \mathrm{rk}^{-1}_{d,1;q}(m-d-1)\rangle & \text{otherwise,} \end{cases}$$

$$\mathrm{rk}^{-1}_{k,q} : q^k \to \mathbb{F}_q^k : m \mapsto (\kappa_{a_0}, \ldots, \kappa_{a_{k-1}}),$$

$$\mathrm{rk}^{-1}_{d,k;q}(m) = \begin{cases} \mathrm{rk}^{-1}_{d,*;q}(m) & \text{if } k = d \\ e^{(k)} + \mathrm{rk}^{-1}_{k,q}(m) & \text{if } m < q^k \\ \mathrm{rk}^{-1}_{d,k+1;q}(m - q^k + 1) & \text{otherwise.} \end{cases}$$

$$\mathrm{shift}_j(m) := \begin{cases} m & \text{if } m < j, \\ m+1 & \text{otherwise.} \end{cases}$$

m	$\mathrm{rk}^{-1}_{2;2}(m)$	$\mathrm{rk}^{-1}_{2;3}(m)$	$\mathrm{rk}^{-1}_{3;2}(m)$
0	⟨1,0,0⟩	⟨1,0,0⟩	⟨1,0,0,0⟩
1	⟨0,1,0⟩	⟨0,1,0⟩	⟨0,1,0,0⟩
2	⟨0,0,1⟩	⟨0,0,1⟩	⟨0,0,1,0⟩
3	⟨1,1,1⟩	⟨1,1,1⟩	⟨0,0,0,1⟩
4	⟨1,1,0⟩	⟨1,1,0⟩	⟨1,1,1,1⟩
5	⟨1,0,1⟩	⟨2,1,0⟩	⟨1,1,0,0⟩
6	⟨0,1,1⟩	⟨1,0,1⟩	⟨1,0,1,0⟩
7		⟨2,0,1⟩	⟨0,1,1,0⟩
8		⟨0,1,1⟩	⟨1,1,1,0⟩
9		⟨2,1,1⟩	⟨1,0,0,1⟩
10		⟨0,2,1⟩	⟨0,1,0,1⟩
11		⟨1,2,1⟩	⟨1,1,0,1⟩
12		⟨2,2,1⟩	⟨0,0,1,1⟩
13			⟨1,0,1,1⟩
14			⟨0,1,1,1⟩

Example of how to enumerate using the rank functions

Example We have $\theta_2(2) = 2^2+2+1 = 7$, $\theta_2(3) = 3^2+3+1 = 13$ and $\theta_3(2) = 2^3+2^2+2+1 = 15$. Table shows the labeling of points of $PG_2(2)$, $PG_2(3)$ and $PG_3(2)$.

Conversely, we have

$$\begin{aligned}
\mathrm{rk}_{3;2}(\langle 1,1,1,1\rangle) &= 4\\
\mathrm{rk}_{3;2}(\langle 1,1,0,0\rangle) &= 3+2-1+\frac{0}{1}+\mathrm{rk}_{1,2}((1))\\
&= 4+1=5\\
\mathrm{rk}_{3;2}(\langle 0,1,1,1\rangle) &= 2+\frac{6}{1}+\mathrm{shift}_6^{-1}(\mathrm{rk}_{3,2}((0,1,1)))\\
&= 8+\mathrm{shift}_7^{-1}(6)\\
&= 8+6=14\\
\mathrm{rk}_{2;3}(\langle 2,2,1\rangle) &= 2+\frac{6}{2}+\mathrm{shift}_4^{-1}(\mathrm{rk}_{2,3}((2,2)))\\
&= 5+\mathrm{shift}_4^{-1}(8)\\
&= 5+7=12
\end{aligned}$$

$$\mathrm{rk}_{k,q}:\mathbb{F}_q^k \to q^k : (\kappa_{a_0},\dots,\kappa_{a_{k-1}}) \mapsto m,$$

$$\mathrm{shift}_j(m) := \begin{cases} m & \text{if } m<j,\\ m+1 & \text{otherwise.}\end{cases}$$

$$\mathrm{rk}_{d;q}(\langle u\rangle) = \begin{cases} k & \text{if } \langle u\rangle = \langle e^{(k)}\rangle\\ d+1 & \text{if } \langle u\rangle = \langle 1,\dots,1\rangle\\ d+2-k+q\theta_{k-2}(q)+\mathrm{rk}_{k,q}\left(\frac{u_0}{u_k},\dots,\frac{u_{k-1}}{u_k}\right) & \text{if } k=\mathrm{lc}(u)<d\\ 2+q\theta_{d-2}(q)+\mathrm{shift}^{-1}_{\theta_{d-1}(q)}\left(\mathrm{rk}_{d,q}\left(\frac{u_0}{u_d},\dots,\frac{u_{d-1}}{u_d}\right)\right) & \text{if } \mathrm{lc}(u)=d.\end{cases}$$

m	$\mathrm{rk}^{-1}_{2;2}(m)$	$\mathrm{rk}^{-1}_{2;3}(m)$	$\mathrm{rk}^{-1}_{3;2}(m)$
0	$\langle 1,0,0\rangle$	$\langle 1,0,0\rangle$	$\langle 1,0,0,0\rangle$
1	$\langle 0,1,0\rangle$	$\langle 0,1,0\rangle$	$\langle 0,1,0,0\rangle$
2	$\langle 0,0,1\rangle$	$\langle 0,0,1\rangle$	$\langle 0,0,1,0\rangle$
3	$\langle 1,1,1\rangle$	$\langle 1,1,1\rangle$	$\langle 0,0,0,1\rangle$
4	$\langle 1,1,0\rangle$	$\langle 1,1,0\rangle$	$\langle 1,1,1,1\rangle$
5	$\langle 1,0,1\rangle$	$\langle 2,1,0\rangle$	$\langle 1,1,0,0\rangle$
6	$\langle 0,1,1\rangle$	$\langle 1,0,1\rangle$	$\langle 1,0,1,0\rangle$
7		$\langle 2,0,1\rangle$	$\langle 0,1,1,0\rangle$
8		$\langle 0,1,1\rangle$	$\langle 1,1,1,0\rangle$
9		$\langle 2,1,1\rangle$	$\langle 1,0,0,1\rangle$
10		$\langle 0,2,1\rangle$	$\langle 0,1,0,1\rangle$
11		$\langle 1,2,1\rangle$	$\langle 1,1,0,1\rangle$
12		$\langle 2,2,1\rangle$	$\langle 0,0,1,1\rangle$
13			$\langle 1,0,1,1\rangle$
14			$\langle 0,1,1,1\rangle$

Presentation Outiline

- Representing Graphically the Orbits
- The orbit Data Structure
- Enumerating points of projective vector spaces using ranks
- ✓ **Lexicographic ordering**
- Arranging points of projective spaces in a order trees
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- Constructing all (n,k, q, dmin≥ 3) using Orderly Generation of codes (canonical subsets can be computed

Lexicographic order

Let $(X, \leq)$ be a totally ordered set

$\wp(X)$=$\{A \mid A \subseteq X\}$

$\wp_k(X)$=$\{A \mid A \subseteq X, |A| = k\}$

Let $A \subseteq X$, then $A = \{a_0, a_1, \ldots, a_{m-1}\}_<$, $that\ is,\ \ a_0 < a_1 < \cdots < am_{-1}$

For subsets $A = \{a_0, a_1, \ldots, am_{-1}\}_<$ and $B = \{b_0, b_1, \ldots, b_{n-1}\}_<$ of the totally ordered set X, we say that $A \preccurlyeq B \Leftrightarrow \begin{cases} \exists\, r < \min(m, n) : a_i = bi\ for\ i \in r\ and\ ar < br, or \\ m \leq n \quad and \quad a_i = bi\ for\ i \in m \end{cases}$

Lexicographical in an order Tree

Let $X = \{x_0, x_1, \ldots, x_{n-1}\}_<$ *be a finite totally ordered set. Let ,* $\preccurlyeq$ *be the lexicographical order on* $P(X)$*. Then we can build an order tree* $T_{\preccurlyeq}$ *, as follows:*

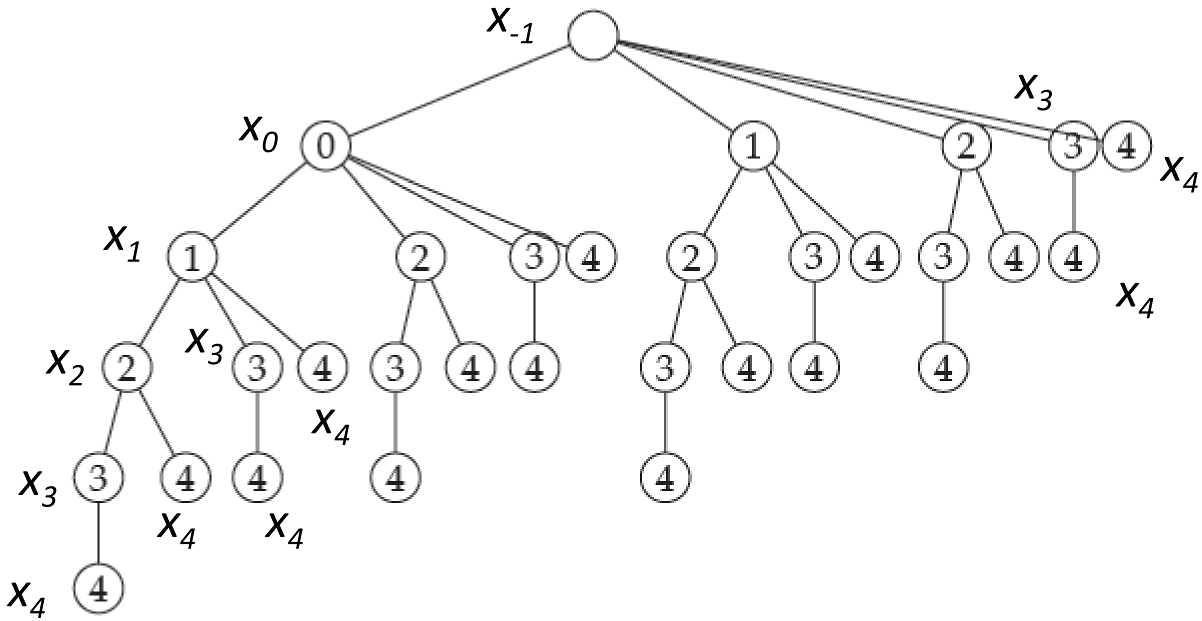


Fig. 9.3 Order tree of subsets of {0, 1, 2, 3, 4}   n=5

Subsets of {0,1,2,3,4} ordered Lexicographically:

{0,1,2,3,4}<{0,1,2,4}<{0,1,3,4}<{0,1,4}<{0,2,3,4}<{0,2,4}<{0,3,4}<{0,4}<{1,2,3,4}<{1,2,4}<{1,3,4}<{1,4}<{2,3,4}<{2,4}<{3,4}<{4}

Presentation Outline

- Representing Graphically the Orbits
- The orbit Data Structure
- Enumerating points of projective vector spaces using ranks
- Lexicographic ordering
- ✓ **Arranging points of projective spaces in a order trees**
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- Constructing all (n,k, q, dmin≥ 3) using Orderly Generation of codes (canonical subsets can be computed

Lexicographical order Tree

Level i & i-subsets

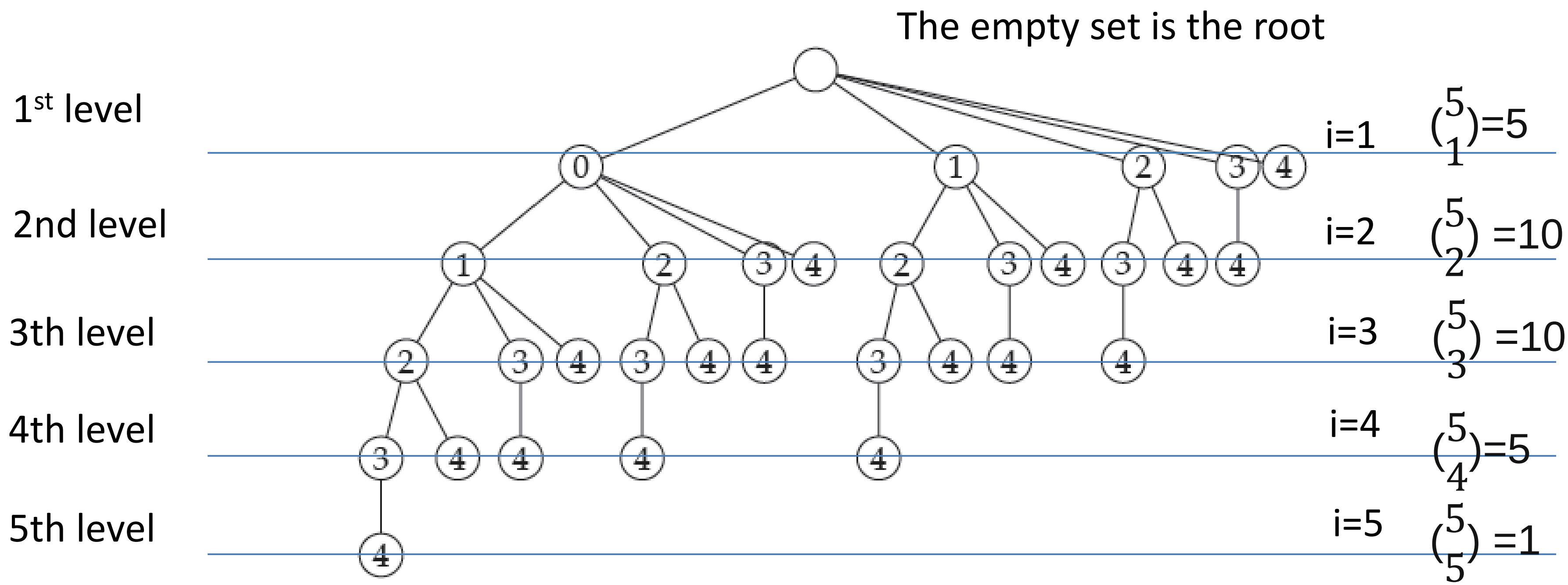


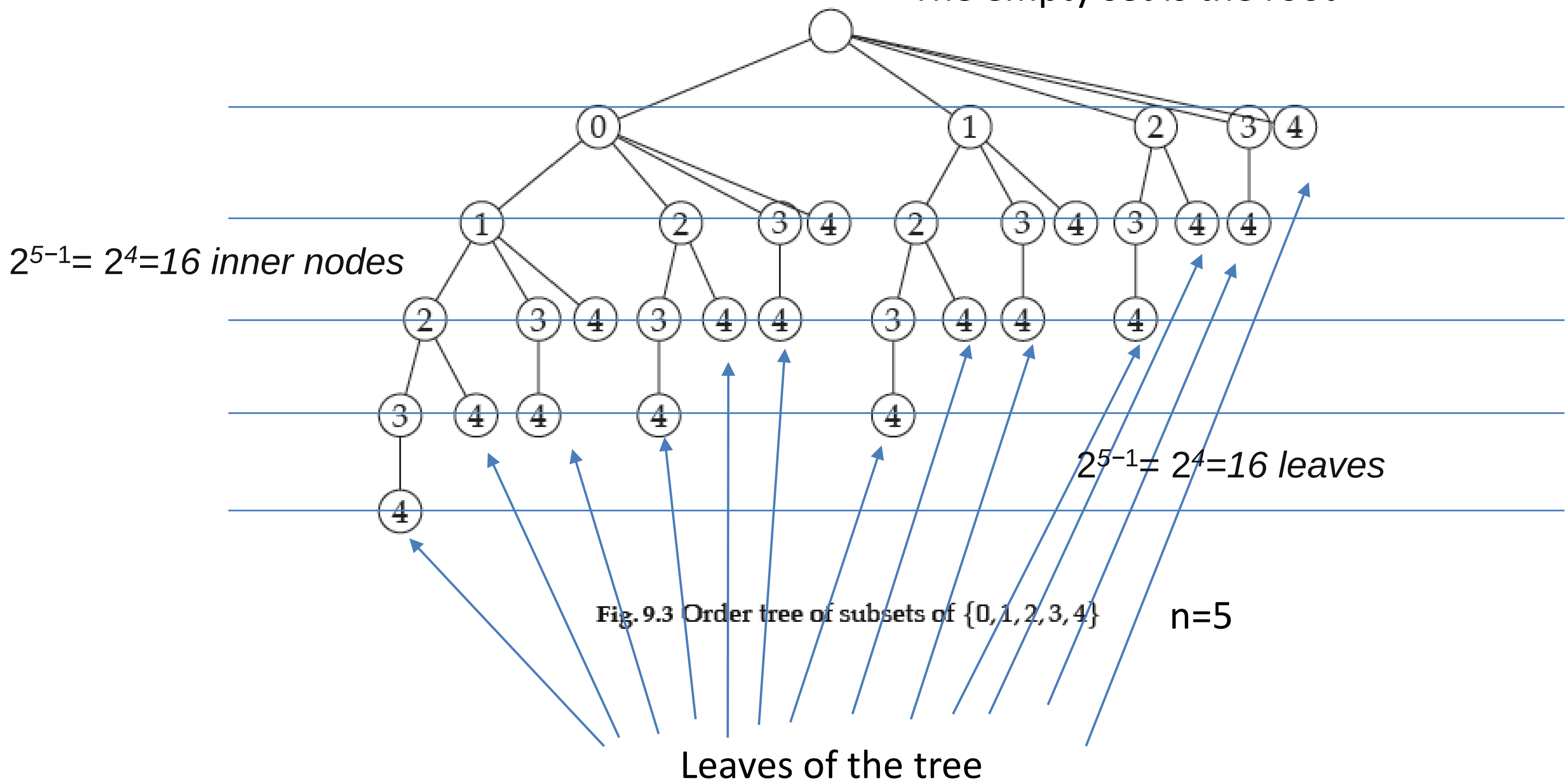
Fig. 9.3 Order tree of subsets of $\{0, 1, 2, 3, 4\}$ n=5

The nodes at level i correspond to i-subsets of X, and hence there are $\binom{n}{i}$ of them.

Lexicographic order tree

Number of leaves & inner nodes

The empty set is the root



The tree has 2^{n-1} leaves corresponding to the subsets of X which contain x_{n-1}.
The tree has 2^{n-1} inner nodes corresponding to the subsets of X which do not contain x_{n-1}.

Lexicographic order Tree

The labels

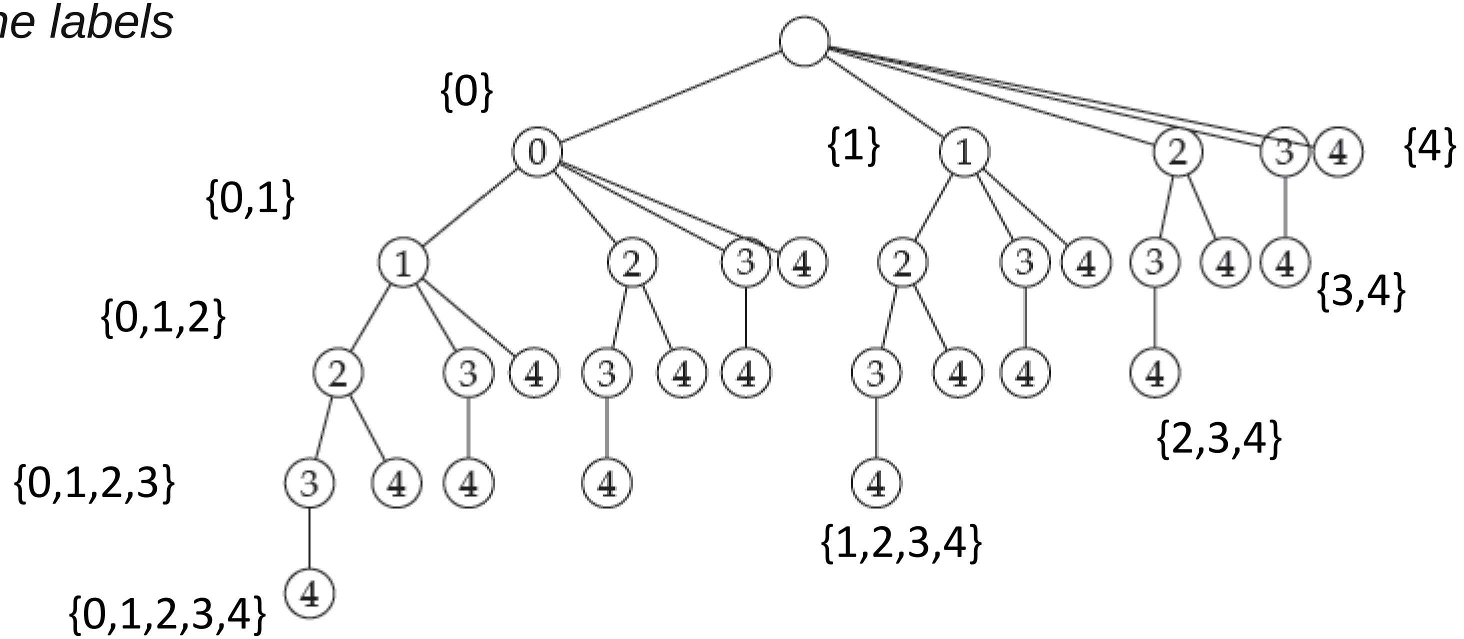


Fig. 9.3 Order tree of subsets of {0, 1, 2, 3, 4}

we label the nodes by the largest element of the set which they represent

For every node of the tree, the corresponding set is the union of the labels along the path leading to that node. Moreover, the labels are encountered in ascending order along this path

Lexicographic order tree

leftmost and Right most leaves

The empty set is the root

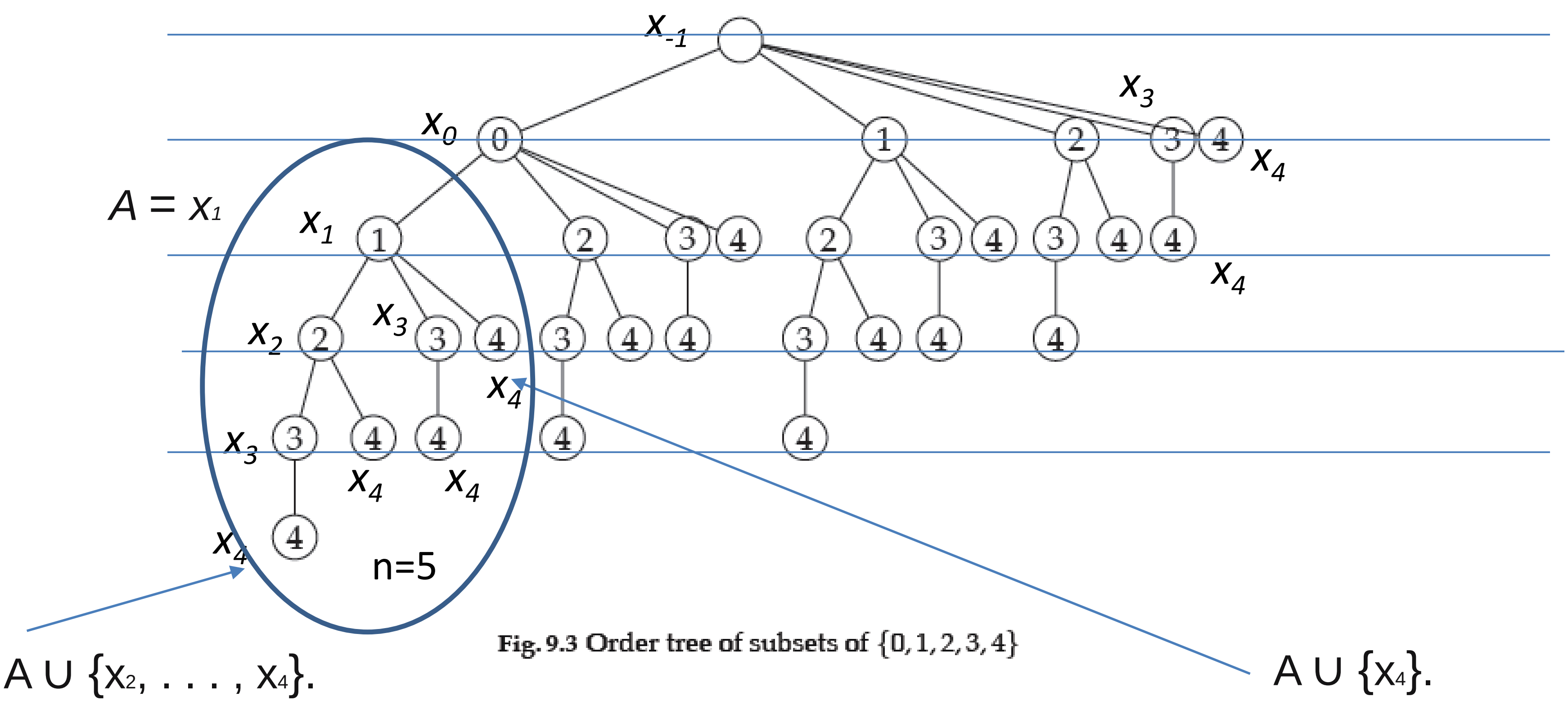


Fig. 9.3 Order tree of subsets of {0, 1, 2, 3, 4}

Let A be a subset with max *A* = x_i *(put i* = −1 *if A* = ∅*). The leftmost leaf in the subtree rooted at A is the set A* ∪ {x_{i+1}, . . . , x_{n-1}}*. The rightmost leaf in the subtree rooted at A is the set A* ∪ {x_{n-1}}.

Lexicographic order Tree

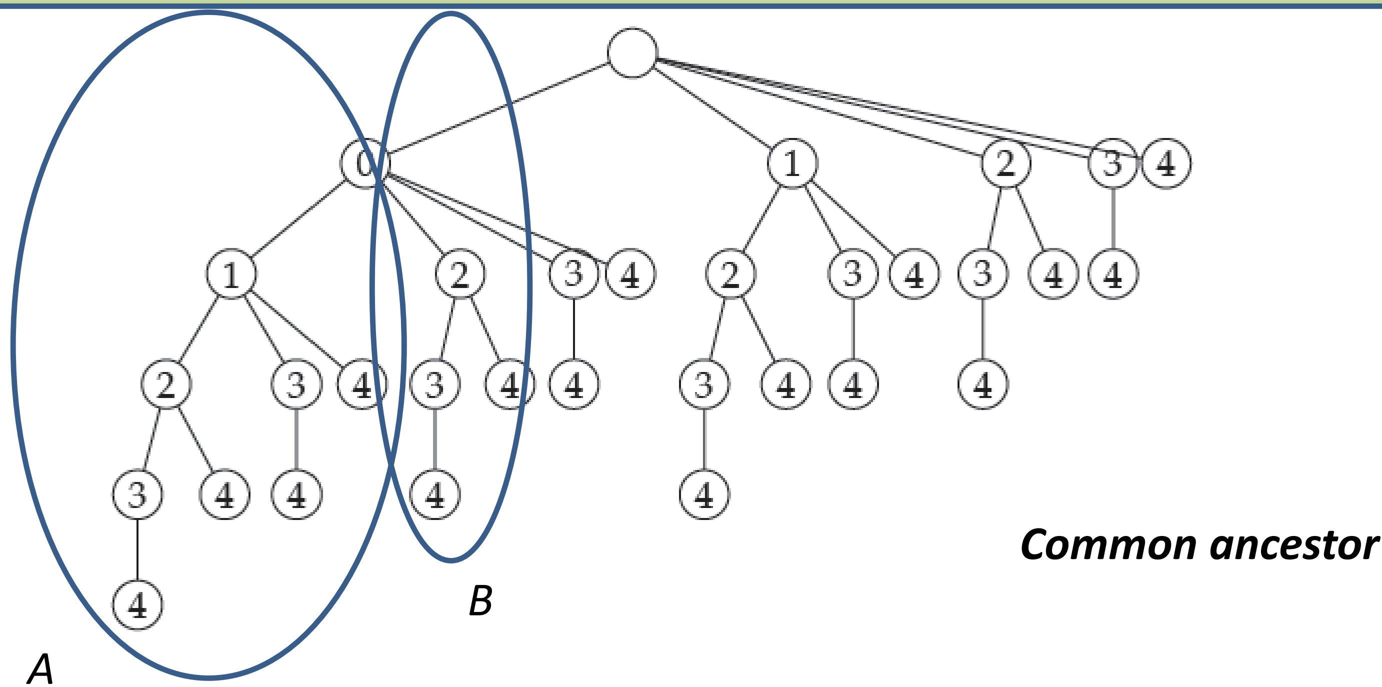


Fig. 9.3 Order tree of subsets of $\{0, 1, 2, 3, 4\}$

For A, B ⊆ X, a common ancestor of A and B corresponds to a prefix of A∩ B and vice-versa. The immediate common ancestor is the prefix of A∩ B which is largest in size.

Two subtrees rooted at sets A and B (with A, B ⊆ X) are equal in shape and labeling of the nodes if and only if max *A* = max *B*.

Lexicographic order Tree

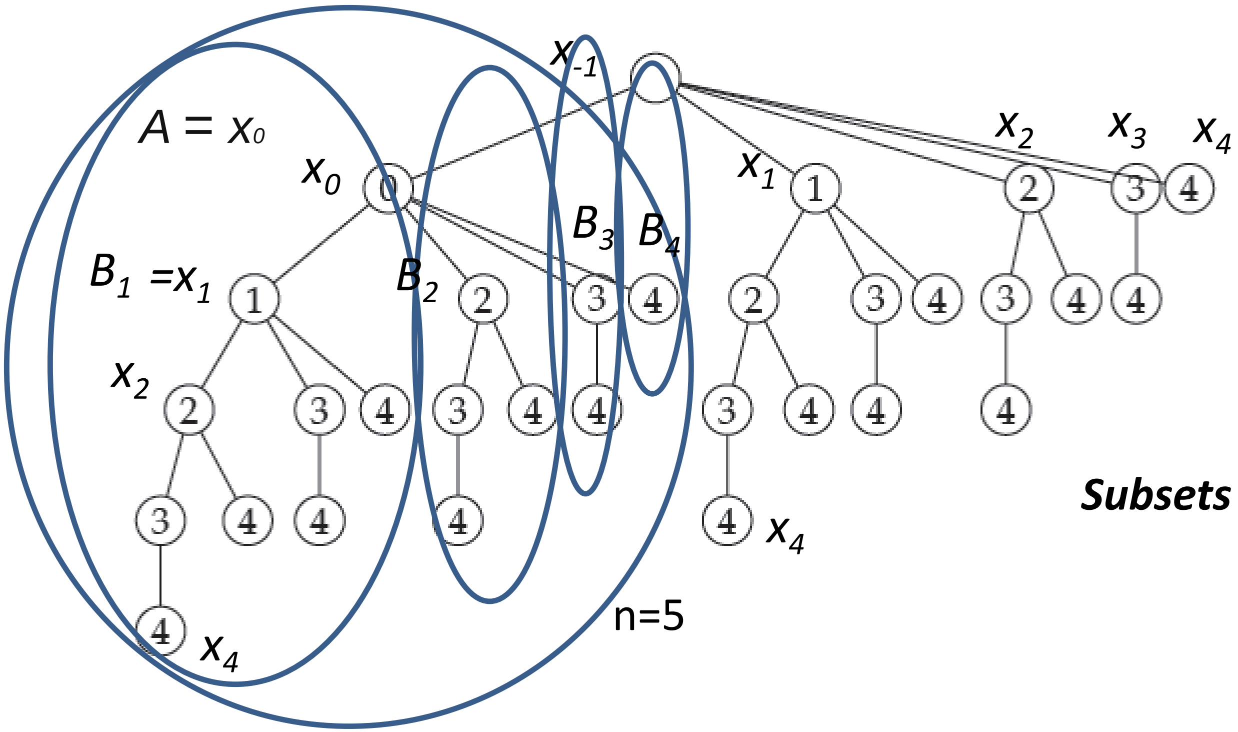


Fig. 9.3 Order tree of subsets of {0, 1, 2, 3, 4}

Subsets of subtrees

The subtree rooted at a set $A \subseteq X$ consists of the subsets $B \subseteq X$ for which A is a prefix of B. If max $A = x_i$*, there are* $2^{n-1} - i$ *such nodes.*

In particular, the subtree

whose root is $\{x_i\}$ (i.e. the tree which is rooted at the i-th descendant of the global root), contains all subsets $A \subseteq X$ with min $A = x_i$*. There are* $2^{n-1} - i$ *such sets.*

Traversing the nodes of the tree using **depth first search strategy**

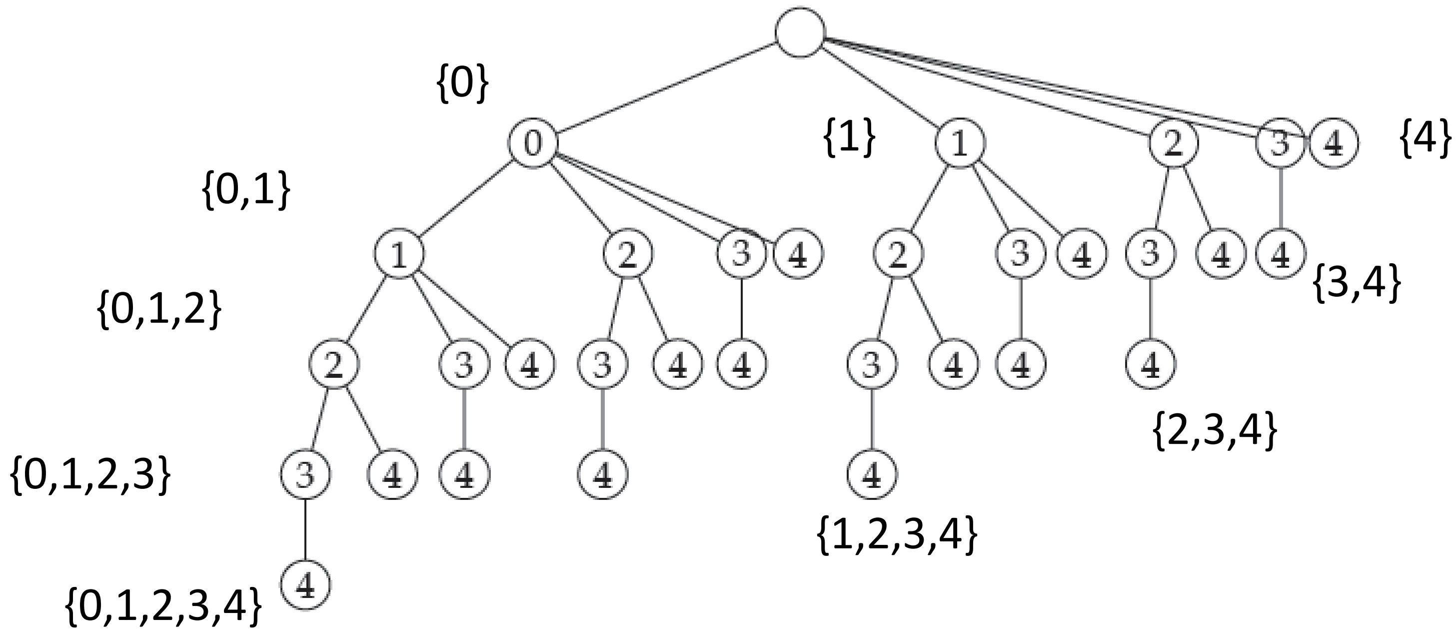


Fig. 9.3 Order tree of subsets of {0, 1, 2, 3, 4}

{0}	{0,1}	{0,1,2}	{0,1,2,3}	{0,1,2,3,4}
		{0,1,3}	{0,1,3,4}	{0,1,4}
	{0,2}	{0,2,3}	{0,2,3,4}	{0,2,4}
	{0,3}	{0,3,4}	{0,4}	……………………

A ≼ B if and only if either B is a descendant of A or the branch containing B is to the right of the branch containing A among the siblings of the immediate common ancestor of A and B.

If the order tree is traversed in depth first search, the subsets are encountered in lexicographic order.

Lexicographic order

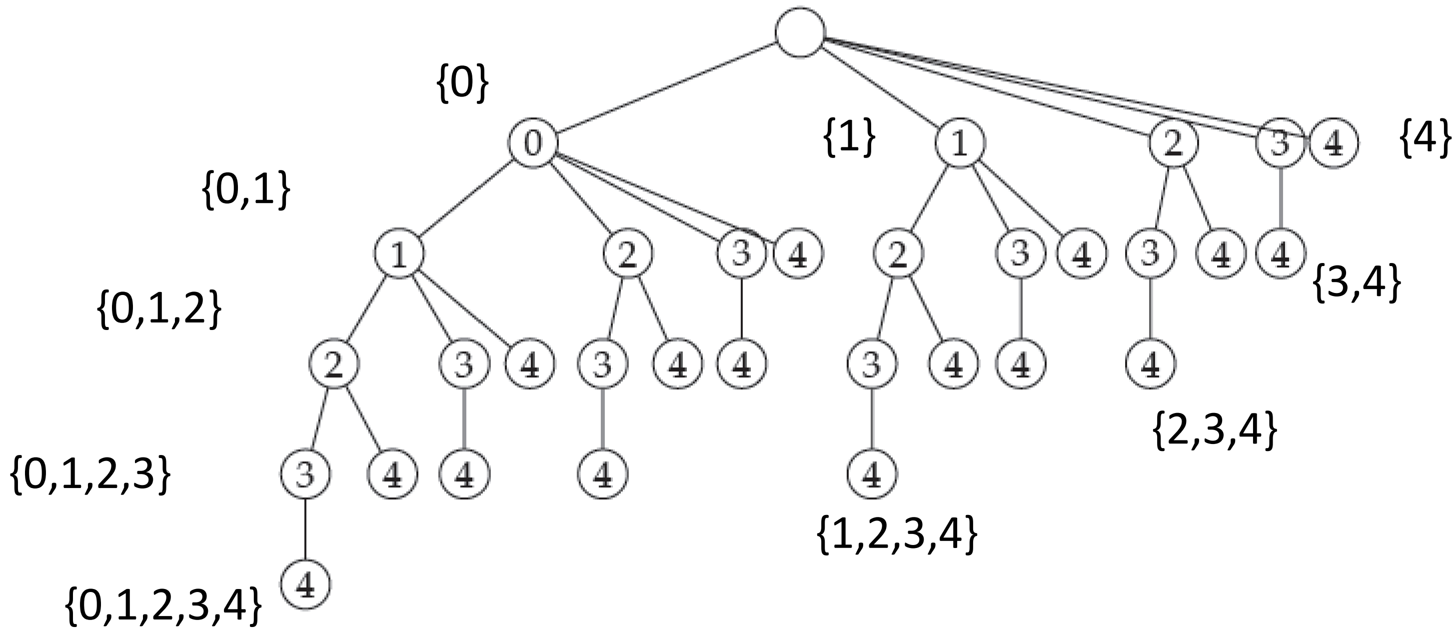


Fig. 9.3 Order tree of subsets of $\{0, 1, 2, 3, 4\}$

{0} {1} {2} {3} {4}

{0,1} {0,2} {0,3} {0,4} {1,2} {1,3} {1,4} {2,3} {2,4} {3,4}

{0,1,2} {0,1,3} {0,1,4} {0,2,3} {0,2,4} {0,3,4} {1,2,3} {1,2,4} {1,3,4} {2,3,4}

{0,1,2,3} {0,1,2,4} {0,1,3,4} {0,2,3,4} ....

Traversing the nodes of the tree using
breath first search strategy

Presentation Outline

- Representing Graphically the Orbits
- The orbit Data Structure
- Enumerating points of projective vector spaces using ranks
- Lexicographic ordering
- Arranging points of projective spaces in a order trees
- ✓ **Special Rank and unrank functions for subsets of powersets of Ranks in Order trees**
- Constructing all (n,k, q, dmin≥ 3) using Orderly Generation of codes (canonical subsets can be computed

rank and unrank functions for the Powerset of a finite set.

Lemma *Let* $X = \{x_0, x_1, \ldots, x_{n-1}\}_<$ *be a totally ordered finite set of n elements.*

For a set $A \subseteq X$ *define* $\mathrm{rk}_X : P(X) \longrightarrow 2_n$:

$$A \longrightarrow \begin{cases} 0 \text{ if } A = \emptyset, \\ |A| + \sum_{x_i \in X \setminus A,\ x_i < \max A} 2^{n-1-i} \text{ otherwise} \end{cases}$$

This function is one-to-one and onto. Its inverse is the unrank function, defined as

$$\mathrm{rk}^{-1}{}_X(r) := \mathrm{rk}^{-1}{}_X(r, 0),$$

where

$$\mathrm{rk}^{-1}{}_X(r,m) := \emptyset \text{ if } r = 0,$$

while for $0 < r < 2^{n-m}$ *we have*

$$\mathrm{rk}^{-1}{}_X(r,m) := \begin{cases} \{x_m\} \cup \ \mathrm{rk}^{-1}{}_X(r-1, m+1) \text{ if } 2^{n-1-m} \geq r, \\ (r - 2^{n-1-m}, m+1)\ \mathrm{rk}^{-1}{}_X \ \text{ if } 2^{n-1-m} < r. \end{cases}$$

rank and unrank functions for the set of subsets of a finite set.

Example For $X = \{0, \ldots, 4\}$ as above, we have

$$\mathrm{rk}_X(\{1,3,4\}) = 3 + 2^{5-1-0} + 2^{5-1-2} = 23,$$

$$\begin{aligned}
\mathrm{rk}_X^{-1}(23) &= \mathrm{rk}_X^{-1}(23,0) \\
&\overset{16\le 23}{=} \mathrm{rk}_X^{-1}(7,1) \\
&\overset{8\ge 4}{=} \{1\} \cup \mathrm{rk}_X^{-1}(6,2) \\
&\overset{4\le 6}{=} \{1\} \cup \mathrm{rk}_X^{-1}(2,3) \\
&\overset{2\ge 2}{=} \{1,3\} \cup \mathrm{rk}_X^{-1}(1,4) \\
&\overset{1\ge 1}{=} \{1,3,4\} \cup \mathrm{rk}_X^{-1}(0,5) \\
&= \{1,3,4\},
\end{aligned}$$

The tree rooted at {0} has 16 nodes,

the tree rooted at *{1, 2}* brings in another 4 nodes

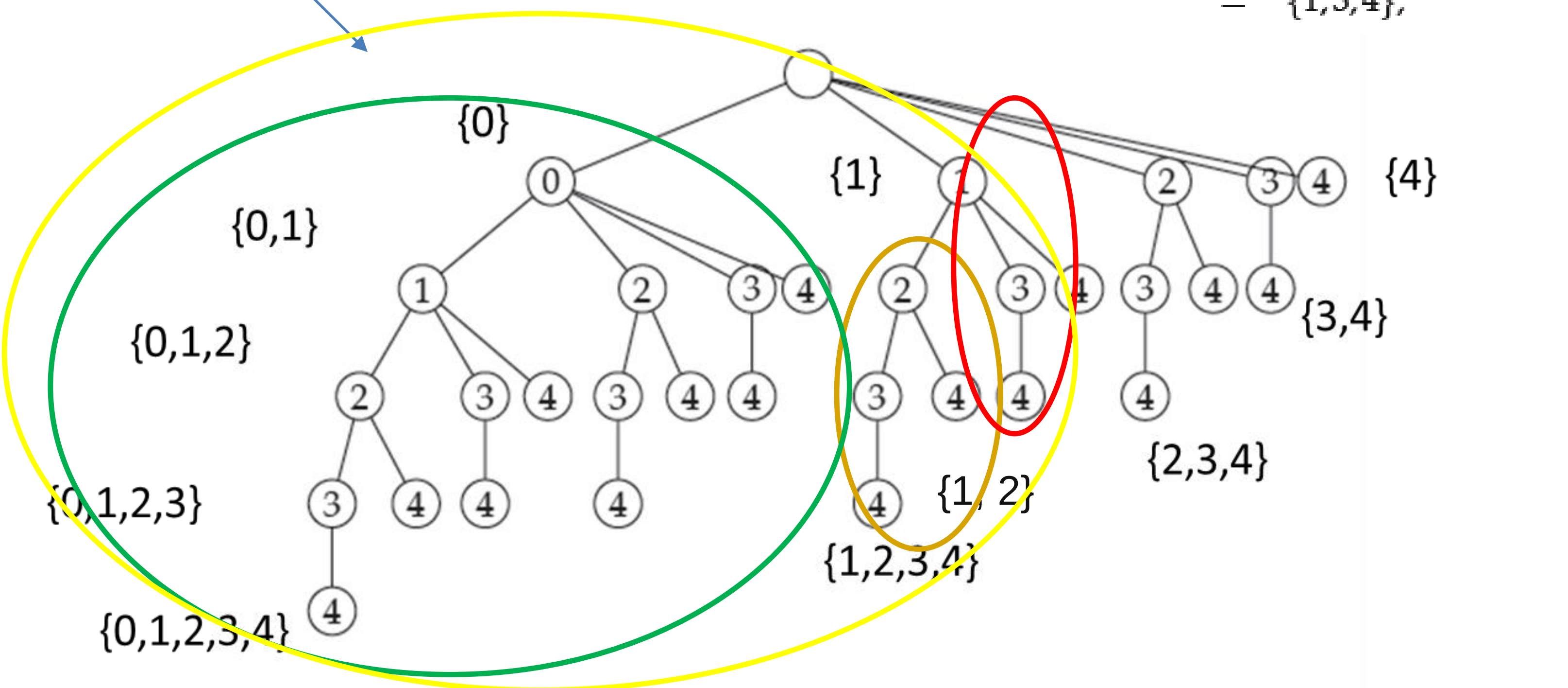


Fig. 9.3 Order tree of subsets of $\{0,1,2,3,4\}$

rank and unrank functions for the set $P_k(X)$ of k-subsets of X, where k is some fixed integer with $0 \le k \le |X|$.

Lemma *Let* $X = \{x_0, x_1, \ldots, x_{n-1}\}_<$ *be a totally ordered finite set of n elements. Let k be an integer with* $0 \le k \le n$*. Define a function, the rank function of* $P_k(X)$ *to the set of integers* $\binom{n}{k}$ *as follows. For a k-subset* $A = \{x_{a0}, x_{a1}, \ldots, x_{ak-1}\}_<$*, put*

$$\mathrm{rk}_{X,k} : P_k(X) \to \binom{n}{k} \quad : A \to \sum_{i=0}^{k-1} \sum_{j=a_{i-1}+1}^{a_i - 1} \binom{n-1-j}{k-1-i}$$

where $a_{-1} := -1$*. The function* $\mathrm{r}^{k}{}_{X,k}$ *is one-to-one and onto.*

Its inverse is the function

$\mathrm{rk}^{-1}{}_{X,k}$, *which is given by* $\mathrm{rk}^{-1}{}_{X,k}(r) = \mathrm{r}^{k-1}{}_{X,k}(r, 0)$,

where

$\mathrm{r}^{k-1}{}_{X,k}(r,m) := \emptyset$ *if* $k = 0$,

Example

Example For $X = \{0, \ldots, 4\}$ as above, we have

$$\mathrm{rk}_{X,3}(\{1,3,4\}) = \binom{5-1-0}{3-1-0} + \binom{5-1-2}{3-1-1} = \binom{4}{2} + \binom{2}{1} = 8,$$

$$\begin{aligned}
\mathrm{rk}_{X,3}^{-1}(8) &= \mathrm{rk}_{X,3}^{-1}(8,0) \\
&\overset{\binom{5-1-0}{3-1}=6\leq 8}{=} \mathrm{rk}_{X,3}^{-1}(2,1) \\
&\overset{\binom{5-1-1}{3-1}=3>2}{=} \{1\} \cup \mathrm{rk}_{X,2}^{-1}(2,2) \\
&\overset{\binom{5-1-2}{2-1}=2\leq 2}{=} \{1\} \cup \mathrm{rk}_{X,2}^{-1}(0,3) \\
&\overset{\binom{5-1-3}{2-1}=1>0}{=} \{1,3\} \cup \mathrm{rk}_{X,1}^{-1}(0,4) \\
&\overset{\binom{5-1-4}{1-1}=1>0}{=} \{1,3,4\} \cup \mathrm{rk}_{X,0}^{-1}(0,5) \\
& \{1,3,4\},
\end{aligned}$$

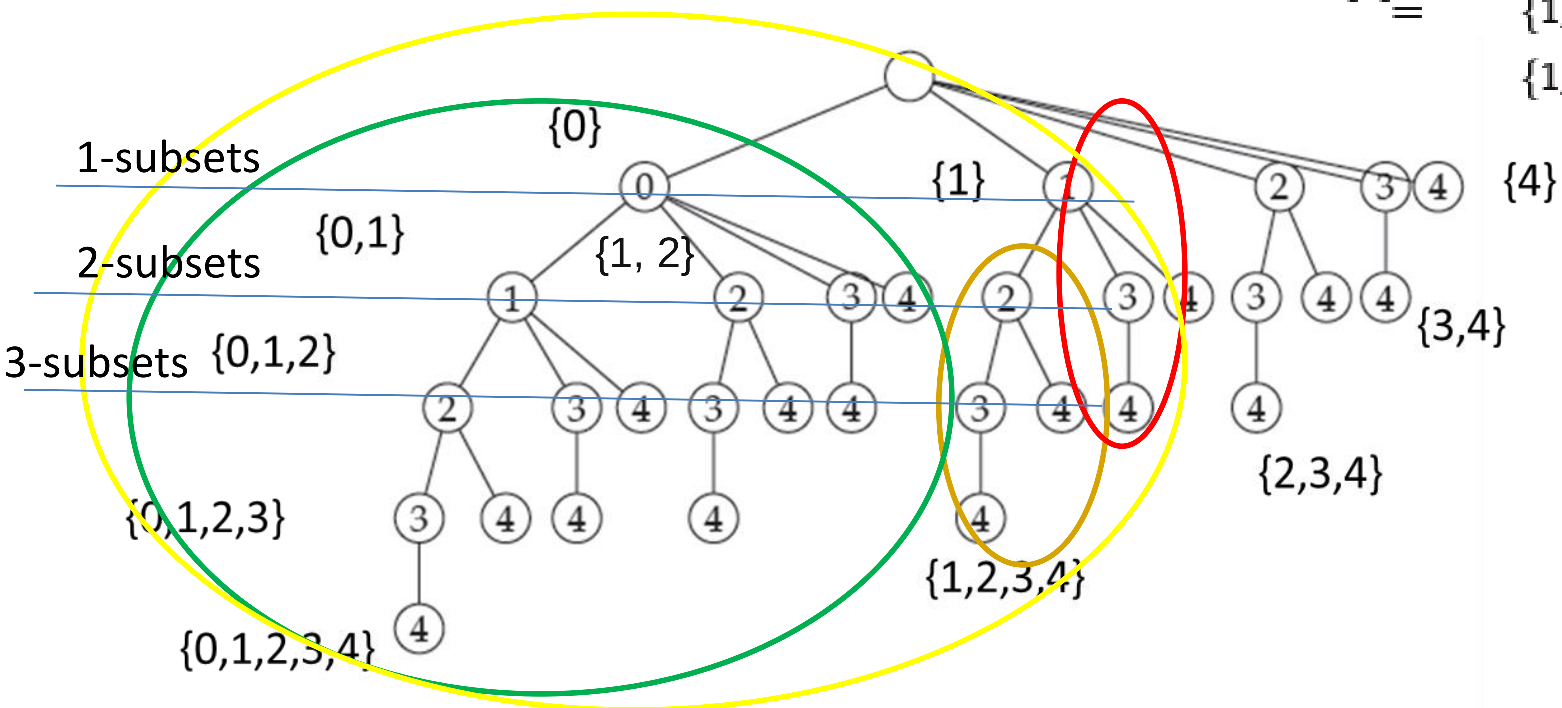


Fig. 9.3 Order tree of subsets of $\{0,1,2,3,4\}$

Presentation Outline

- Representing Graphically the Orbits
- The orbit Data Structure
- Enumerating points of projective vector spaces using ranks
- Lexicographic ordering
- Arranging points of projective spaces in a order trees
- Special Rank and unrank functions for subsets of powersets of Ranks in Order trees
- ✓ **Constructing all (n,k, q, dmin$\geq$ 3) using Orderly Generation of codes (canonical subsets can be computed**

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Picking and Admissible n-set
From the projective Space

In Order to apply theorem 10) construct the linear (n,k) linear codes

using the orbits of n sets,

which **d** $_{min}$ -1 subsets are all in general position

$$PG\boldsymbol{L}_{n\text{-}k}(\mathbf{q})\backslash\backslash\binom{PG_{n-k-1}(\mathbf{q})}{\boldsymbol{n}}$$

We need to verify whether the n-subset of PG_{n-k-1}(q)
has $\text{dmin} - 1$ points independent

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Test function for independence of points taken from n-set

Verifying that dmin-1 points are independent

For this purpose we use a Testing function

$$f(S) = \begin{cases} 1 \;\; if\ any\ dmin-1\ points\ of\ S\ are\ independent \\ 0\ otherwise \end{cases}$$

We need to verify that two important properties hold

$$f(S) = f(Sg)\ \ \forall g \in G, \forall S \subseteq X$$
$$f(S) = 1 \;\Rightarrow f(T) = 1, \forall\, T \subseteq S \subseteq X$$

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Test function for independence of points taken from n-set

We the help of the test function we define a set

That contains only the codes of our interest

The ones of size n

of just independent vectors

$Y_{n,k,dim,q} = P_n^{(f)}(PG_{n-k-1}(\mathbf{q})) = \{S \subseteq PG_{n-k-1}(\mathbf{q})\} \mid |S| = n, f(S)=1\}$

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Connection between Canonical representatives

And Systematic generator matrices

Lemma

Consider action of G$\geq PGLk(q)$.

Let X be a totally ordered set using functions

$rk^{-1}_{d;q} : \theta_d(q) \to PG_d(q)$ $rk_{d;q} : PG_d(q) \to \theta_d(q)$

Let A:=$\{\langle u^{(0)\,T}\rangle, \ldots, \langle u^{(n-1)\,T}\rangle\}_<$

Be a canonical orbit representative

Let $\Gamma(A) = (u^{(0)\,T} | \ldots | u^{(n-1)\,T})$

Be its generator matrix

The following conditions are equivalent

1. The rank of $\Gamma(A)$ is r

2. $\langle u^{(i)}\rangle = \langle e^{(i)}\rangle$ for i $\in r$ and

$\langle u^{(i)}\rangle = \langle e^{(0)}, \ldots, e^{(r-1)}\rangle$ for j=r,…,n-1

3. $\langle u^{(i)}\rangle = \langle e^{(i)}\rangle$ for i $\in r$ and $\langle u^{(r)}\rangle \neq \langle e^{(r)}\rangle$

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Connection between Canonical representatives

And Systematic generator matrices

Corollary

Let A:=$\{\langle u^{(0)\top}\rangle, \ldots, \langle u^{(n-1)\top}\rangle\}_<$

Be a canonical orbit representative

For an orbit of

$PGL_k(q)$ acting on n-subset of PG_{k-1}**(q)**

Then the matrix $\Gamma(A) = (u^{(0)\top} | \ldots | u^{(n-1)\top})$

Is systematic

a **systematic code** is any error-correcting code in which the input data is embedded in the encoded output.
When the generator matrix is in standard form, the code *C* is systematic in its first *k* coordinate positions.

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Computation of the Canonical Transversal

We compute the orbits of

G= $PGL_{n-k}(q)$\\Y $_{i,k,dim,q}$=$P_n^{(f)}(PG_{i-k-1}(q))$

Where *i* goes from 0 to *n*

This gives rise to

(I,≥i-n+k,≥ dmin,q)-codes

This only for i≥n-k,

At each step the canonical transversal T_i

Is computed

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Tree Graphic Representation
of the Canonical
Transversal

$$T_{\leq n} = \bigcup_{i=0}^{n} T_i$$

Is the tree of canonical representatives

The leaves at depth end

Comprise the isometry classes of codes.

The nodes in the tree are labeled

By the largest element of the set.

The nodes display the ranks of

The projective points rather

Than the points themselves

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

Computation of Construction Of the Codes

The codes are constructed as follows

1st Given orbit representatives

A:=$\{\langle u^{(0)\top}\rangle,\ldots,\langle u^{(s-1)\top}\rangle\}_<$

2nd form the check matrix (ΔA)

S=$\{p_0,p_1,\ldots p_{n-1}\}$ n generating points $p_i \in PG_{n-k-1}(q)$

Determine the Check matrix

$\Delta = (b_{i,j}) \in Fq^{\,n-k\times n}$

3rd Δ may not be *uniquely defined.*

This can be fixed if A be ordered

Increasingly, Not freely. Also we

Choose only representatives that

Are in standard form

(the rightmost non zero coordinate is 1)

4th If the rank of Δ is r then we have

Found an (n,n-r,≥d,q) –code. (n-r≥ k)

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin≥ 3

To obtain the generator matrix :

$\Delta(A) is\ systematic\ provided\ that\ A\ is$

The lexicographically least element in its orbit

If r is determined as the index for which

$\langle u^{(i)} \rangle$=$\langle e^{(i)} \rangle$ for $\mathrm{i} = 0, \ldots, r-1$ and $\langle u^{(r)} \rangle \neq \langle e^{(r)} \rangle$

Then the rank of $\Delta(A)$ is r

Thus $\Delta(A)$=$\begin{pmatrix} I_r & M \\ 0 & 0 \end{pmatrix}$

For some r $\times$ $(n-r)$ - matrix M

Then

$\Gamma(A)$=$(-M^{\top} \quad I_{n-r})$

Constructing a all (n,k)codes over a finite field F_q whose minimum distance is at least dmin, where dmin$\geq$ 3

Example

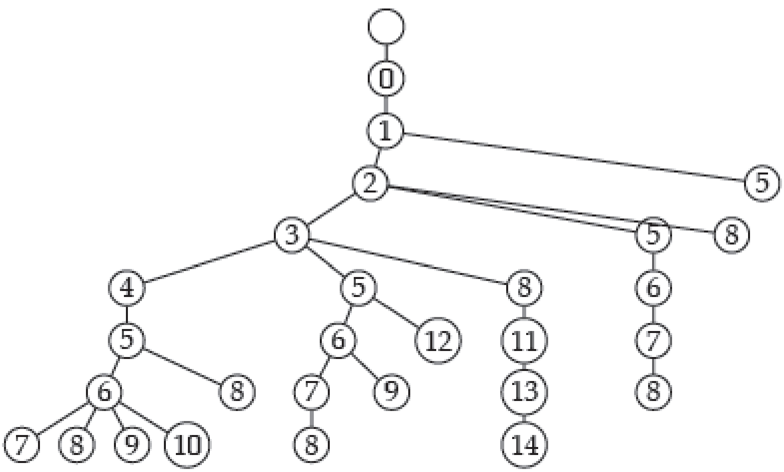


Fig. 9.4 Orbits of $PGL_4(2)$ on $\mathcal{P}_{\leq 8}(PG_3(2))$

Table 9.2 Binary $(8, 4, \geq 3)$-codes

A	$\Delta(A)$	$\Gamma(A)$	d
$\{0,1,2,3,4,5,6,7\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&1&0\\ 0&1&0&0&1&1&0&1\\ 0&0&1&0&1&0&1&1\\ 0&0&0&1&1&0&0&0 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&1&1&1&0&0&0\\ 1&1&0&0&0&1&0&0\\ 1&0&1&0&0&0&1&0\\ 0&1&1&0&0&0&0&1 \end{array}\right)$	3
$\{0,1,2,3,4,5,6,8\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&1&1\\ 0&1&0&0&1&1&0&1\\ 0&0&1&0&1&0&1&1\\ 0&0&0&1&1&0&0&0 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&1&1&1&0&0&0\\ 1&1&0&0&0&1&0&0\\ 1&0&1&0&0&0&1&0\\ 1&1&1&0&0&0&0&1 \end{array}\right)$	3
$\{0,1,2,3,4,5,6,9\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&1&1\\ 0&1&0&0&1&1&0&0\\ 0&0&1&0&1&0&1&0\\ 0&0&0&1&1&0&0&1 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&1&1&1&0&0&0\\ 1&1&0&0&0&1&0&0\\ 1&0&1&0&0&0&1&0\\ 1&0&0&1&0&0&0&1 \end{array}\right)$	3
$\{0,1,2,3,4,5,6,10\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&1&0\\ 0&1&0&0&1&1&0&1\\ 0&0&1&0&1&0&1&0\\ 0&0&0&1&1&0&0&1 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&1&1&1&0&0&0\\ 1&1&0&0&0&1&0&0\\ 1&0&1&0&0&0&1&0\\ 0&1&0&1&0&0&0&1 \end{array}\right)$	3
$\{0,1,2,3,5,6,7,8\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&0&1\\ 0&1&0&0&1&0&1&1\\ 0&0&1&0&0&1&1&1\\ 0&0&0&1&0&0&0&0 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&0&0&1&0&0&0\\ 1&0&1&0&0&1&0&0\\ 0&1&1&0&0&0&1&0\\ 1&1&1&0&0&0&0&1 \end{array}\right)$	3
$\{0,1,2,3,8,11,13,14\}$	$\left(\begin{array}{cccc\|cccc} 1&0&0&0&1&1&1&0\\ 0&1&0&0&1&1&0&1\\ 0&0&1&0&1&0&1&1\\ 0&0&0&1&0&1&1&1 \end{array}\right)$	$\left(\begin{array}{cccc\|cccc} 1&1&1&0&1&0&0&0\\ 1&1&0&1&0&1&0&0\\ 1&0&1&1&0&0&1&0\\ 0&1&1&1&0&0&0&1 \end{array}\right)$	4