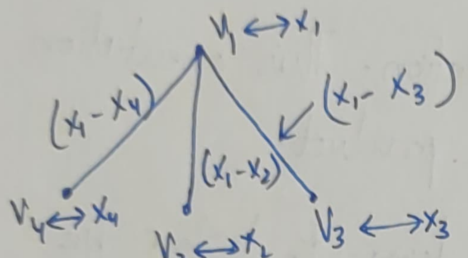
Combinatorial Nullstellensatz:

Let G be a graph with vertex set $V = \{v_1, v_2, \ldots v_n\}$. Set $X = (x_1, \ldots x_n)$

The adjacency polynomial of G is the multivariate polynomial

$$A(G, X) = \prod_{i<j} \{(x_i - x_j) : v_i v_j \in E\}$$



$$A(G, X) = (x_1 - x_2) \cdot (x_1 - x_3) \cdot (x_1 - x_4)$$

→ If there is a proper vertex coloring of the graph, and we consider these colors as numbers and substitute x_i with color given to i^{th} vertex, $x_i - x_j \neq 0$ as i & j^{th} vertex wont have same color. $A(G, X)$ → Non zero value ⇒ proper valid coloring

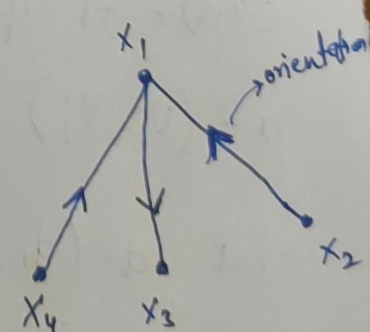
→ Zero ⇒ Not a proper coloring.

→ Expanding the polynomial:

$$(x_1 - x_2)(x_1 - x_3)(x_1 - x_4) = (x_1^2 - x_1 x_3 - x_2 x_1 - x_2 x_3)(x_1 - x_4)$$

$$= x_1^3 - x_1 x_3 x_4 - x_2 x_1^2 - x_2 x_3 x_1 - x_1 x_3 x_4 - x_4 x_1^2$$

"m" edges ⇒ 2^m terms.

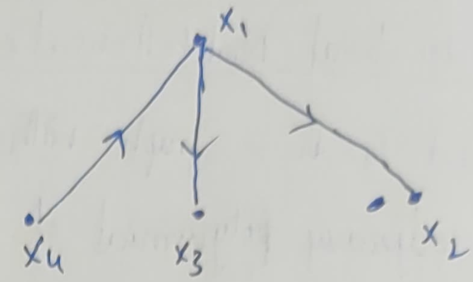


$x_2 x_1 x_4$ ⇒ x_2 from the first term
x_1 from the middle term
x_4 from the third term

x_1, x_2, x_4 outdegree = 1

→ Each monomial corresponds to orientation on the graph, giving a direction to each edge of the graph.

$$x_1^2 x_4 \Rightarrow \left.\begin{array}{l} x_1 \text{ from } 1^{st} \text{ term} \\ x_1 \text{ from } 2^{nd} \text{ term} \\ x_4 \text{ from } 3^{rd} \text{ term} \end{array}\right\}$$



x_1 out degree $= 2$ (x_1^2)

x_4 out degree $= 1$ (x_4)

→ Each monomial corresponds to an orientation. This orientation is wrt to each constituent term of the product.

→ When we are orienting the edge from lower to higher we are picking the +ve term & from higher to lower we are picking the -ve term

$$x_1^2 x_4 \Rightarrow \left.\begin{array}{lll} x_1 \text{ from } 1^{st} \text{ term} & \rightarrow & (\text{lower}) +ve \\ x_1 \text{ from } 2^{nd} \text{ term} & \rightarrow & (\text{lower}) +ve \\ x_4 \text{ from } 3^{rd} \text{ term} & \rightarrow & \text{higher } (-ve) \end{array}\right\} \begin{array}{l} + \cdot + \cdot - \\ = - \end{array}$$

→ Let D be an orientation of G. Then $\sigma(D) = \prod\{\sigma(a) : a \in A(D)\}$

$\sigma(a) = +1$ if $a = (v_i, v_j)$ $i < j$ & $\sigma(a) = -1$ if $a = (v_i, v_j)$ with $i > j$

→ Let $d = (d_1, d_2, \ldots d_n)$ be a sequence of non-negative integers whose sum is m. We define the weight of d by:

$$w(d) = \sum \sigma(D)$$

where sum is taken over all orientations D of G whose out degree sequence is d.

→ In the expansion of the polynomial:

$x_1^{d_1} \; x_2^{d_2} \; \ldots \; x_n^{d_n}$ ⟶ degree seq

m → degree of each monomial

$\therefore d_1 + d_2 + \ldots d_n = m$.

→ Adding the coefficients of all monomials is summing up the signs of the corresponding orientations.

$$x^d = \prod_{i=1}^{n} x_i^{d_i}$$

$$A(G, x) = \sum_{d} w(d) x^d$$ → $w(d)$ need not only be +1 or −1

→ We are interested when this polynomial evaluates to non-zero (proper vertex coloring)

→ Let f be a non-zero polynomial over a field F in the variables $X = (x_1, x_2, \ldots x_n)$ of degree d_i in x_i for $1 \le i \le n$. Let L_i be a set of $d_i + 1$ elements of F, $1 \le i \le n$. Then there exists $t \in L_1 \times L_2 \times \ldots L_n$ such that $f(t) \neq 0$. (proof by induction)

↓

If the polynomial has only 1 variable, if you have $d+1$ roots (dist) where d is the degree of the polynomial, then when one of them is substituted for x, we get a non zero value.

$$f(x_1, x_2, \ldots x_n) = f_0(x_1, x_2, \ldots x_{n-1}) x_n^0 + f_1(x_1 \ldots x_{n-1}) x_n^1 + f_2(x_1, x_2 \ldots x_{n-1}) x_n^2 + \ldots \ldots f_{d_n}(x_1, \ldots x_{n-1}) x_n^{d_n}$$

If we are given d_n+1 distinct values, then x_n can get a value that evaluates the polynomial to be non zero.

<u>The combinatorial Null~~s~~tellensatz:</u>

Let f be a polynomial over a field F in the variables $x=(x_1, x_2, x_3, \dots x_n)$. Suppose that the total degree of f is $\sum_{i=1}^{n} d_i$ and that the coefficients in f of $\prod x_i^{d_i}$ non-zero. Let L_i be the set of d_i+1 elements of F, $1 \le i \le n$. Then there exists a $t \in L_1 \times L_2 \times \dots \times L_n$ such that $f(t) \neq 0$.

↳ We arent saying x_1's highest degree is d_1 or x_2's highest degree is d_2

↳ d_i is the parameter associated with each x_i

↳ x_i may have degree $> d_i$ but the sum of all degrees of x_i will be $\sum_{i=1}^{n} d_i$

↳ $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ term's coeff must be nonzero.

<u>Proof:</u>

$$f_i = \prod_{t \in L_i} (x_i - t)$$

$|L_i| = d_i + 1$

$f_i \rightarrow$ poly of x_i d_i+1 degree

$$f_i = x_i^{d_i+1} + g_i$$

$g_i \rightarrow$ poly of x_i d_i, degree

for any $t \in L_i$ $f_i(t) = 0$

$\therefore\ 0 = t^{d_i+1} + g_i \Rightarrow t^{d_i+1} = -g_i$

"f" be a polynomial.

$x_i^{d_i+1} \cdot x_i^{\epsilon}$ term $\longrightarrow$ $-g_i \cdot x_i^{\epsilon}$

$\downarrow$ $-g_i$

$\downarrow$ degree $= x_i^{d_i}$

lower degree term

"f" $\xrightarrow[\text{repeatedly substitution}]{}$ "g" where $x_i^{d_i}$ is the degree

$x_1 \rightarrow d_1$

$x_2 \rightarrow d_2$

$\vdots$

$x_n \rightarrow d_n$

$g(t) = f(t)$

$t \in L_1 \times L_2 \times \dots L_d$

for showing $f(t) \neq 0$, we need to show it for $g(t) \neq 0$ for

$t \in L_1 \times L_2 \times \dots L_d$

→ The polynomial will be non-zero if we consider

$C_1 \cdot x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ term

$\downarrow$ Non zero coeffs

→ Not changed in $f \rightarrow g$ conversion.

→ For every other term their degree has reduced

$C_1 \cdot x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ → highest degree term, non zero coeffs

∴ The polynomial has to evaluate a non-zero value for some selection of x_i's.

∴ The resulting polynomial is a non-zero polynomial.

Theorem: Let F be an arbitrary field and $P(x_1, x_2, \ldots x_n)$ be a polynomial in $F[x_1, x_2, \ldots x_n]$. Suppose the degree $(\deg(P))$ of P is $\sum_{i=1}^{n} k_i$, k_i is a non neg integer, and suppose the coefficient of $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ in P is non zero. Then for any subsets $A_1, A_2, \ldots A_n$ of F satisfying $|A_i| \geq k_i + 1$ $\forall i = 1, 2, \ldots n$ there are $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$ $a_n \in A_n$ so that

$$P(a_1, a_2, \ldots a_n) \neq 0.$$

→ We need to find an upper bound on the zero-error capacity that can be achieved using only linear codes for the case when $G = \Gamma(\mathbb{F}_p, S)$ is a cayley graph over the additive group $\mathbb{F}_p$ & a symmetric set S.

→ Upper bound is proven by an application of the polynomial method.

→ Symmetric set:

→ A non empty subset S of a group G is said to be symmetric if $S = S^{-1}$ where $S^{-1} = \{s^{-1} : s \in S\}$

→ So wrt additive group structure $S = -S = \{-s : s \in S\}$

→ Linear Independence Number:

For any Graph G with $V(G) = \mathbb{F}_q$ and any $k \geq 1$, the linear independence number of G^k denoted as $\alpha_{lin}(G^k)$ is the largest independent set I_L of G^k that is linear

$$I_L = \{(x, Ax),\ x \in \mathbb{F}_q^m\} \text{ for some matrix } A \in \mathbb{F}_q^{(k-m)\times m}$$

$m \rightarrow$ no of msg bits

$k \rightarrow$ no of encoded bits (codeword size)

$x \rightarrow$ column vector $m \times 1$

$Ax \rightarrow (k-m) \times 1$ vector

$A \rightarrow (k-m) \times m$ vector

Testing it out:

Suppose $F_q = F_5 = \{0,1,2,3,4\}$ $\quad K=1$

$\alpha(G) \rightarrow$ largest independent set I_L of G

since $k=1$, $1 \leq m \leq 1 \Rightarrow m=1$

$x \in F_5$, $A \in F_5^{0\times 1}$ doesnt make sence.

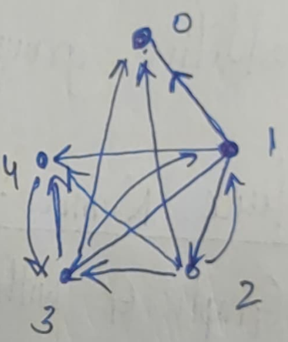
$K=2$

$\alpha(G^2) \rightarrow$ largest Independent set I_L of G^2

$m=1$ $\quad x \in F_q^{1\times 1} \Rightarrow x \in \{0,1,2,3,4\}$

$A \in F_5^{1\times 1} \quad \Rightarrow A \in \{0,1,2,3,4\}$

$Ax = \{0,1,2,3,4\}$



→ Let F_q be a finite field, $S \subset F_q$ is symmetric under addition.

→ Cayley graph $G = \Gamma(F_q, S)$

$V(G) = F_q$

$(V, U) \in G$ iff $(V - U) \in S$

Try it out:

$F_q = F_5 = \{0, 1, 2, 3, 4\}$

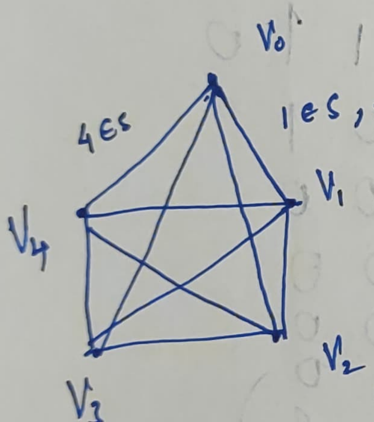
$0 \to$ additive identity

$-i \to$ additive inverse $\forall i \in F_5$

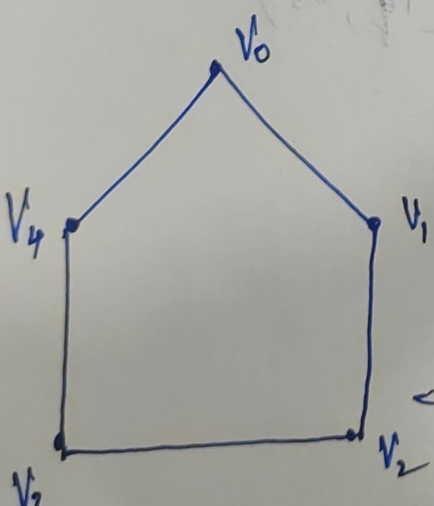
$S_1 = \{1, 4, 2, 3\}$

$S_2 = \{1, 4\}$, $S_3 = \{2, 3\}$

$G = \Gamma(F_q, S_1)$



If we take S_1, $G \to$ complete graph.



$G = \Gamma(F_q, S_2)$

→ C_5 graph

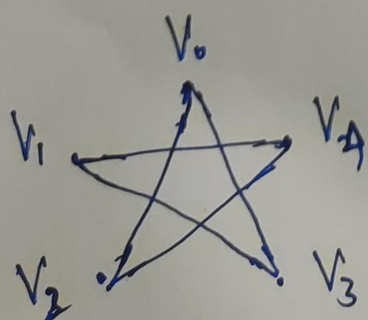
$(U, V) = 1$ or 4

Circulant matrix.

$$
\begin{array}{c|ccccc}
 & V_0 & V_1 & V_2 & V_3 & V_4 \\
\hline
V_0 & 0 & 1 & 0 & 0 & 1 \\
V_1 & 1 & 0 & 1 & 0 & 0 \\
V_2 & 0 & 1 & 0 & 1 & 0 \\
V_3 & 0 & 0 & 1 & 0 & 1 \\
V_4 & 1 & 0 & 0 & 1 & 0
\end{array}
$$

⟷ circulant graph

circulant matrix



$G = \Gamma(F_q, S_3)$

$U - V = 2$ or 3

(U, V)

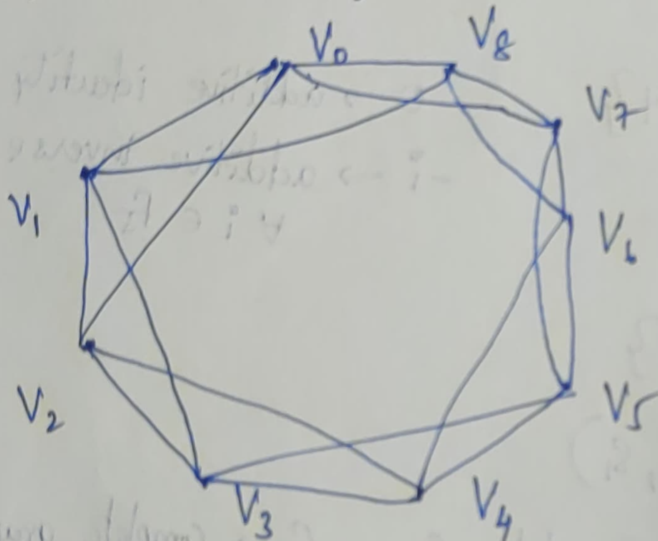
$$
\begin{array}{c|ccccc}
 & V_0 & V_1 & V_2 & V_3 & V_4 \\
\hline
V_0 & 0 & 0 & 1 & 1 & 0 \\
V_1 & 0 & 0 & 0 & 1 & 1 \\
V_2 & 1 & 0 & 0 & 0 & 1 \\
V_3 & 1 & 1 & 0 & 0 & 0 \\
V_4 & 0 & 1 & 1 & 0 & 0
\end{array}
$$

$F_q \longrightarrow F_9$ $\quad q = 3^2$ (prime power)

$S_1 = \{1,2,3,4,5,6,7,8\}$ $\quad F_9 = \{0,1,2,3,4,5,6,7,8\}$

$S_2 = \{1,2,7,8\}$ $\quad S_3 = \{3,4,5,6\}$

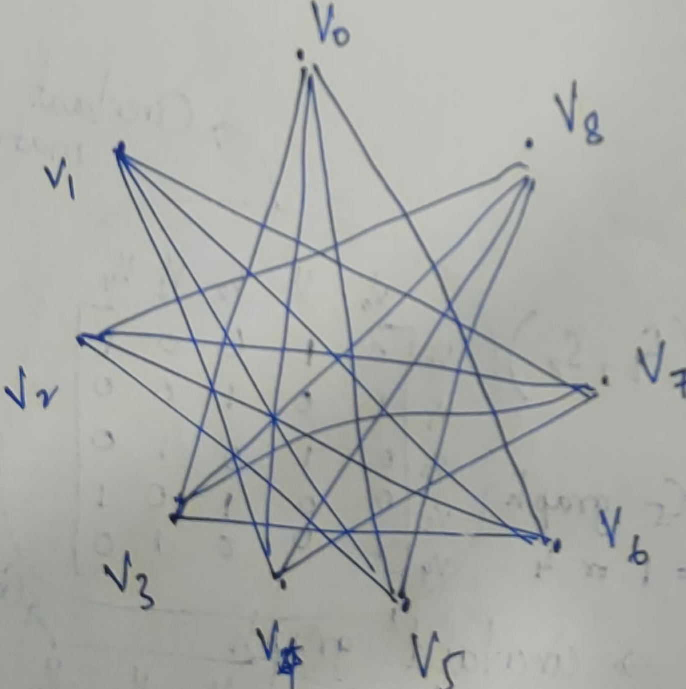
$G = \Gamma(F_9, S_2)$



$\Gamma(F_9, S_2)$

	V_0	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8
V_0	0	1	1	0	0	0	0	1	1
V_1	1	0	1	1					
V_2	~~0~~	1	0	1					
V_3	0	1	1	0					
V_4	0	0	1						
V_5	0	0	0						
V_6	0	0	0						
V_7	1	0	0						
V_8	1	1	0						

$\Gamma(F_q, S_3)$

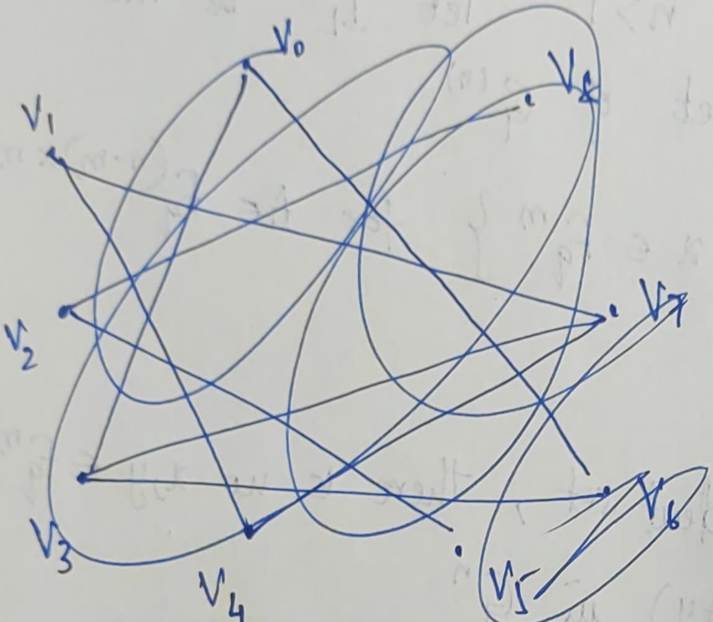


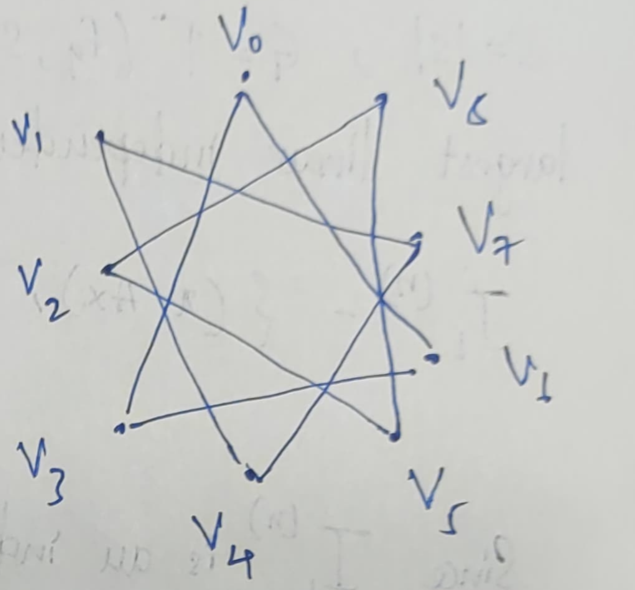
→ When q = prime, additive group of F_q is cyclic & this cayley graph is a circulant graph. Also, any circulant graph of prime order is such a cayley graph.

↳ seems to be working for $q=9$

↙ Non prime odd value

$S_4 = \{3, 6\}$ $G = \Gamma(F_9, S_4)$





Circulant matrix:

	V_0	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8
V_0	0	0	0	1	0	0	ϕ	0	0
V_1	0	0	0	0	1	0	0	ϕ	0
V_2	0	0	0	0	0	1	0	0	1
V_3	1	0	0	0	0	0	1	0	0
V_4	0	1	0	0	0	0	0	1	0
V_5	0	0	1	0	0	0	0	0	1
V_6	1	0	0	1	0	0	0	0	0
V_7	0	1	0	0	1	0	0	0	0
V_8	0	0	1	0	0	1	0	0	0

Theorem:

Let F_q be any finite field and $S \subseteq F_q \setminus \{0\}$ be any symmetric set. Then

$$\Theta(\Gamma(F_q, S)) \leq q^{1-\frac{|S|}{q-1}}$$

Proof:

$s = |S|$, $G = \Gamma(F_q, S)$ $n > 1$ let $I_L^{(n)}$ be the largest linear independent set of $G^{(n)}$

$$I_L^{(n)} = \{(x, Ax), \text{ for } x \in F_q^m\} \text{ for } A \in F_q^{(n-m) \times m}$$

Since $I_L^{(n)}$ is an independent set, there is no $x, y \in F_q^m$ such that $(x, Ax) \sim (y, Ay)$ in G^n

$\downarrow$

No 2 messages x, y give the same codeword.
(No confusion vertex $\Rightarrow$ Independent set)

No $z \in F_q^m$ such that $(z, Az) \sim 0^n$ in G^n

$\downarrow$

$z \to m \times 1$ column matrix

$A \in F_q^{(n-m) \times m}$

$\therefore Az \to (n-m) \times 1$ matrix as $m \geq 1$, order of $Az \neq n$

$\Rightarrow 0^n \longrightarrow$ Not possible.

Testing stuff out:

$G \to C_5$ $\quad \alpha(G) = \{1, 3\}$ $\longrightarrow$ for example.

$G^2 = C_5 \boxtimes C_5$

$\downarrow$

codeword of length $= 2$

We know for C_5^2, The MIS : $\{$ "11" , "23" , "30" , "04" , "42" $\}$

(x_1, Ax_1) $\quad (x_2, Ax_2)$ $\quad (x_3, Ax_3)$ $\quad (x_4, Ax_4)$ $\quad (x_0, Ax_0)$

If $x \in F_q^m$ where $m = 1$

$x = 1$, $Ax = 1$ $\quad A = 1$ $\quad {}^{1 \times 1}$

$x = 2$, $Ax = 3$ $\quad A = 4$ $\quad A = F_q$

$x = 3$, $Ax = 0$ $\quad A = 0$

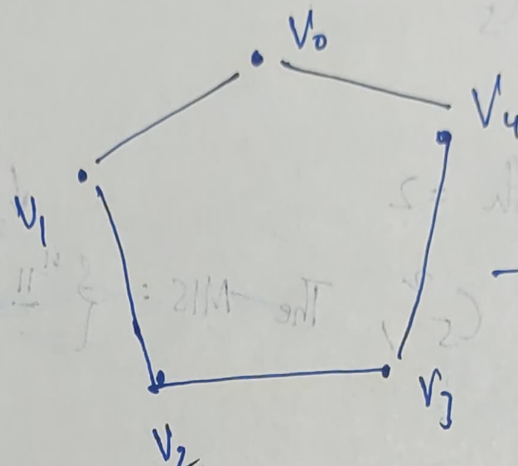
$x = 4$, $Ax = 2$ $\quad A = 3$

$x = 0$, $Ax = 4$ $\quad A = 0$

$F_q \to F_5 = \{0, 1, 2, 3, 4\}$

$S \subseteq F_q - \{0\} \Rightarrow S = \{\underset{s}{1}, \underset{s^{-1}}{4}\}$ additive group.

$\Gamma(F_q, S) =$



$\longrightarrow C_5$ graph.

Acc to the theorem,

$1 - \frac{2}{4}$ $\le \sqrt{5}$

$\Theta_{lin}\, T(F_q, S) \le 5$

$s = |S| = 2$, $n = 2$

$G^n = C_5 \boxtimes C_5$

$S_0 = \{0, 1, 4\}$

$(S_0)^m - \{0^m\} \Rightarrow$ for $m = 1$,

$z \in \{S_0\} - \{0\}$

$\Rightarrow S$

$z \in S$.

$D = S_0^{\,c} = F_q - S_0 = \{2, 3\}$