Chapter No. 2

GALOIS FIELD AND FINITE GEOMETRIES

In this chapter , we discuss about the Galois Field and finite Geometries. In the section 2.1 , we give some definitions and elementry properties of Galoies field. In the section 2.2 we discuss about the finite projective Geometry and in section 2.3 we discuss about finite Euclidean Geometry along with comparison of it with FG(m,s).

Fisher during his visit to India, in the seminar held under the auspices of the Indian statistical Institute, made a guess that it should be possible to construct experimental designs by using properties of Galois field.

Bose (1938) has shown that his guess was correct. In the construction of factorial designs the properties of Galois field are very useful. We will discuss about the construction of factorial designs by using the properties of Galois field later on. First we discuss about Galois field.

2.1 Definitions And Elementary Properities of Galois Field :

Galois field is a particular type of field, so it is worthwhile to define first, 'field of numbers '.

Definition 2.1.1 : Field :--

Let corrosponding to every pair of elements a, b $\in$ F , there exist two unique determined elements a + b , called the addition of elements and a.b , called the multiplication of elements in F , then the system F is called a 'field '-if the addition and multiplication satisfy the following postulates.

I. $a + b = b + a$, $a . b = b . a$

II. $(a + b) + c = a + (b + c)$, $(ab) c = a (bc)$.

III. There exist two elements 0 and 1 in F such that

$a + 0 = a$ and $a . 1 = a$ for every 'a' in F .

IV. To every $a \neq 0$, there exists an element ($-a$) and an element a^{-1} such that st $a + (-a) = 0$ and $a . a^{-1} = 1$.

The element ' $- a$ ' is called an additive inverse of 'a' and ' a^{-1} ' is called multiplicative inverse or simply inverse of a .

V. $c (a + b) = ca + cb$.

For example, set of all rational numbers , set of all complex numbers, residue modulo p ; where p is primer or power of prime are fields.

Definition 2.1.2 : Galois field :--

A field containing finite number of elements is called as, 'finite field ' or 'Galois field '. A finite field has been derived by Galois Evariste (1811 - 1832), so it is called as , 'Galois Field '.

A Galois field containing s elements is denoted by 'GF(s)' And when s is a prime, the elements of GF(s) are 0, 1, 2, - - - - , s - 1. These elements may be called as the marks of the field.

As an example we consider s = 7 . The elements of GF(7) are 0, 1, 2, 3, 4, 5 and 6. The simplest example of a Galois field is provided by the field of the classes of residue mod p , p - being any prime positive integer.

" Properties Of Galois Field "

Following are the different properties of Galois field :-

1. A rule is made that any positive integer N is equal to the remainder R when N is divided by an positive prime number p .

Then R is written as

$$R = N \bmod p .$$

And a field of such R elements of modulo p - is a Galois field.

2. If p is a prime number then all the four operations of addition, substraction, multiplication and division are possible.

To illusatrate this we take any two elements from GF(7). For instance, suppose 4 and 5 belonging to GF(7) are chosen, then

(i). $4 + 5 = 9 \bmod(7) = 2$,

(ii). $4 - 5 = 6$,

(iii). $4 * 5 = 20 \bmod(7) = 6$,

and (iv) . $4 / 5 = 5$.

It is seen that all the elements ; 2, 6, 6 and 5 are the elements of GF(7) .

3. When any element of a prime modulo is multiplied in turn by its nonzero elements, each time a different product is obtained. This ensures all possible divisions. But when p is non prime, this property does not hold and hence all divisions are not possible. When division is possible, the elements are said to form a Galois field. When division is not possible the multiplicative inverse for that element does not exist. So Galois field does not formed. As an example let us consider elements 3

and 4 from GF(6). Note that multiplicative inverses for 3 and 4 do not exist, so the set of numbers 0, 1, 2, 3, 4, 5 is not closed under the operation of multiplication. Hence for, s = 6 , Galois field does not exist.

4. There is at least one element in every field, different powers of which give the different nonzero elements of the field. Such an element is called the 'Primitive root ' or 'primitive element ' of the GF(s) .

Also, for any element x of GF(s) $x^d = 1$. And if $x = x'$ is a primitive root, then $x'^d \neq 1$, when $d < s - 1$.

As an illustration , we consider GF(7) and check whether 3 is a primitive element or not.

we have ,

$$3^0 = 1 ,\ 3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1.$$

Here, d = s − 1 . Hence , 3 is a primitive element of GF(7).

Again, consider x = 2 . We have ,

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 1 .$$

Here d = 3 < 6 . Hence, 2 is not a primitive element of GF(7).

Also, if we consider x = 5 , we have

$$5^0 = 1,\ 5^1 = 5,\ 5^2 = 4,\ 5^3 = 6,\ 5^4 = 2,\ 5^5 = 3,\ 5^6 = 1 .$$

Hence , 5 is also a primitive element of GF(7). Which implies that, primitive element is not unique. Further, 3 is multiplicative inverse of 5 and both are primitive elements. From this we have the following theorem --

<u>Theorem 2.1.1</u> :- If x is a primitive element of GF(p), then it's multiplicative inverse is also an primitive element of GF(p).

proof :- We shall prove the above theorem by contradiction.

Let x be a primitive element of GF(p) and y is a multiplicative inverse of x .

Hence,

$$x \cdot y = 1 \qquad \text{--------------------} \quad (2.1.1)$$

Suppose, y is not a primitive element, then

$$y^d = 1 , \quad \text{for} \quad d < p - 1.$$

Consider,

$$x^d y^d = x^d$$

$$(x.y)^d = x^d$$

Hence, by equation (2.1.1), we have

$$x^d = 1 , \quad \text{for} \quad d < p - 1 .$$

which implies, x is also not a primitive element, which is a contradiction to the assumption for x is a primitive element.

Hence, we conclude that y is also a primitive element .

***

If , x is a primitive element of GF(p), then all the non-zero elements of GF(p) can be expressed as ,

$$x^0 = 1, x^1 , x^2 , x^3 , x^4 , - - - - , x^{p-1} .$$

And this is called the power cycle of x^1 . For $x^1 = 5$, the power cycle is given as -

$$5^0 = 1, 5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3, 5^6 = 1 .$$

A most general Galois field contains of p^n elements, whear p is a prime positive integer, and n any integer. Two Galois fields with same number of elements are isomorphic. i.e.

structurally identical in such a way that the sum corrosponds to the sum and the product to the product. The Galois field with p^n elements is usually symbolised by $GF(p^n)$.

Let $x_1, x_2, ---, x_{p^n-1}$ be all the nonzero elements of $GF(p^n)$, then

$$ax_1 . ax_2 . --- . ax_{p^n-1} = x_1 . x_2 --- x_{p^n-1}$$

if $a =/= 0$.

Hence,

$$a^{p-1} = 1 \quad \text{----------- (2.1.2)}$$

For all $a =/= 0$ and $a \subset GF(p^n)$.

In general, a Galois field of p^n elements is obtained as follows :

Let $P(x)$ by any given polynomial in x of degree n with coefficients belonging to $GF(p)$ and $F(x)$ by any polynomial in x with integral coefficients. Then $F(x)$ can be expressed as,

$$F(x) = f(x) + p.q(x) + P(x).Q(x) \quad \text{--------- (2.1.3)}$$

Where,

$$f(x) = a_0 + a_1 x + a_2 x^2 + --- + a_{n-1} x^{n-1} \quad \text{.------ (2.1.4)}$$

and the coefficients a_i, ($i = 0, 1, 2, --- n-1$) belong to $GF(p)$. This relaticn may be written as -

$$F(x) = f(x) \bmod \{ p, P(x) \} \quad \text{---------------- (2.1.5)}$$

and we say, $f(x)$ is the residue of $F(x)$ modulo . p and $P(x)$. The functions $F(x)$ that satisfy (2.1.5), when $f(x)$, p and $P(x)$ are kept fixed form a class. If p and $P(x)$ are kept fixed but $f(x)$ is varied, p classes may be formed, since each coefficient in $f(x)$ may take the p values of $GF(p)$. Note that the classes defined by $f(x)$, form a commutative ring, which will be a field if and only if $F(x)$ is irreduciable over GF(p)[Bose (1947)].

The finite field formed by the p^n classes of residues is called a Galois field of order p^n and is denoted by $GF(p^n)$. The function $F(x)$ is said to be a minimum function for generating the elements of $GF(p^n)$. The minimum function need not be unique for $GF(p^n)$. Once a minimum function is found all the nonzero elements of $GF(p^n)$ are given as --

$$x^0 = 1, x^1, x^2, x^3, - - - - , x^{p-1} \quad \text{residue modulo } F(x)$$

and x is a primitive root of the equation $x^{p-1} = 1$. Such an equation having roots as primitive roots is called the 'cyclotomic equation'.

Here main difficulty is to find 'minimum function'. Following are the different steps [Bose(1947)] used to find minimum function for given $GF(p^n)$.

Step 1 :- Divide $x^{p^n-1} - 1$ by the least multiple of all factors like $x^d - 1$, where d is a divisor of $p^n - 1$.

Step 2 :- Obtain the equation

$$\frac{x^{p^n-1} - 1}{x^d - 1} = 0 \qquad \text{---------------- (2.1.6)}$$

The roots of this equation are all the primitive roots of the equation $x^{p^n-1} = 1$. The order of this equation (2.1.6) will be $\Theta(p^n - 1)$, where $\Theta(k)$ denotes the number of positive integrs less than k and relatively prime to it. And let this equation be as, --

$$x^m + a_{m-1} x^{m-1} + - - - + a_0 = 0 \quad \text{------------} \quad (2.1.7)$$

where, m is order of this equation , and a_{m-1} , a_{m-2} , - - a_0 are integers. And this is a cyclotomioc eqution.

Step 3 :- Replace the integers a_i of the left hand side of equation (2.1.7) by their residue classes (a_i) modulo P, and obtain the cyclotomic polynomial ,

$$x^m + (a_{m-1}) x^{m-1} + - - - + (a_0) \quad \text{------------} \quad (2.1.8)$$

Step 4 :- Find the irreduable factor of polynomial (2.1.8).

Let P(x) is that irreduable factor. Then P(x) is a minimum function.

As an example, we find a minimum function for generating the elements of $GF(2^2)$.

Here,

$$n = 2 \quad \text{and} \quad p = 2$$

Hence,

$$F(x) = x^3 - 1 .$$

Step 1 :- We divide $x^3 - 1$ by $x - 1$

$$\text{i.e.} \quad (x^3 - 1)/(x - 1) = x^2 + x + 1 .$$

Step 2 :- The cyclomotic equation is ,

$$x^2 + x + 1 = 0 .$$

Step 3 :- Cyclotomic polynomial is $x^2 + x + 1$.

Step 4 :- Let,

$$x^2 + x + 1 = (ax + b) (cx + d)$$

$$= acx^2 + (bc + ad) x + bd$$

which implies ,

$$ac = 1 \quad \text{--------------} \quad (2.1.9)$$

$$bc + ac = 1 \quad \text{--------------} \quad (2.1.10)$$

$$bc = 1 \quad \text{--------------} \quad (2.1.11)$$

From, equations (2.1.9) and (2.1.11) we get

$$a = c = b = d = 1 .$$

But with these values equation (2.1.10) is not satisfied. So $x^2 + x + 1$ cannot be further factorised. Hence $x^2 + x + 1$ is a irreducible polynomial and is a minimum function for $GF(2^2)$.

With this minimum fLnction, we generate the elements of $GF(2^2)$. If x is a primitive root , the nonzero elements are $x^0 = 1$, $x^1 = x$, $x^2 = x+1$.

Following is a list of some minimum functions that are needed in the construction of designs.

Galois Field	Minimum Functions
2^2	$x^2 + x + 1$
2^3	$x^3 + x^2 + 1$
2^4	$x^4 + x^3 + 1$
3^2	$x^2 + x + 2$
3^3	$x^3 + 2x + 1$
5^2	$x^2 + 2x + 3$
7^2	$x^2 + 6x + 3$.

With the help of Galois field GF(s), we can construct finite geometries such as Finite Projective Geometry and Finite

Euclidean Geometry. We discuss detail about them in the next sections.

2.2 . Finite Projective Geometry :-

From Galois field we can construct a finite projective geometry of m dimensions in the following manner ; where s is prime power i.e. $s = p^n$; p --prime number and n any positive integer.

Consider the ordered set of (m + 1) elements

$$(x_0 , x_1 , x_2 , - - - , x_m) \qquad \text{-------- (2.2.1)}$$

where the x_i's belong to GF(s) and are not all simultaneously zero. This ordered set (2.2.1) may be taken as a point of projective geometry of m dimensions. This projective geometry is denoted by PG(m,s). It is clear that two points (x_0 , x_1 , - - - - - x_m) and (y_0 , y_1 , - - - y_m) are same if and only if,

$$y_i = \rho x_i , \qquad i = 0, 1, 2 - - -, m .$$

where,

ρ is a nonzero element of GF(s). And we may take x_0 , x_1 , - - - x_m as the co-ordinates of point (2.2.1).

Each of x_0 , x_1 , - - -, x_m can be chosen in s different ways and not all x_i's are simulataneously zero. So the total number of points in PG(m,s) is ,

$$s^{m+1} - 1 .$$

Since, two points (x_0 , x_1 , - - , x_m) and (y_0 , y_1 , - - , y_m)

are same when $y_i = \rho x_i$; $i = 0, 1, 2, - - - m$ and $\rho \neq 0$.

so, ρ can take $s - 1$ values. Hence, the number of distinct ponts in PG(m,s), denoted by q_m are

$$q_m = \frac{s^{m+1} - 1}{s - 1} \qquad \text{----------} \quad (2.2.2).$$

For $m = 0$, we get $q_0 = 1$. For justification, we can cosider PG(3,3). The possible number of distinct points for all x_i's not simultaneously equal to zero are enumerated as --

(0,0,1), (1,0,0), (1,0,1), (1,0,2), (0,1,0),

(0,1,1), (0,1,2), (1,1,0), (1,1,1), (1,1,2),

(1,2,0), (1,2,1), (1,2,2).

These are in all 13 .

By, using the equation (2.2.2), we get

$$q_2 = \frac{3^3 - 1}{3 - 1}$$

$$= 13$$

Hence the verification ,

Definition 2.2.1 : Flat :-

All the points which satisfy a set of (m - 1), (1 < m) independent linear homogeneous equations

$$\left.\begin{array}{l}
a_{10} x_0 + a_{11} x_1 + a_{12} x_2 + - - - + a_{1m} x_m = 0 \\
a_{20} x_0 + a_{21} x_1 + a_{22} x_2 + - - - + a_{2m} x_m = 0 \\
- \\
a_{m-1.0} x_0 + a_{m-1.1} x_1 + - - - + a_{m-1.m} x_m = 0
\end{array}\right\} \quad (2.2.3)$$

may be said to form a l --dimensional subspace, or briefly , a l -flat in PG(m,s). The equations may be said to represent this flat. It is clear that [Raghav Rao (1971)] any other set of $m - l$ independant equations, obtained by linear combinations of the equations, in system of equations (2.2.3) , will have same set of solutions, and hence it will represent the same l -flat. Note that the number of independent points lying on the l -flat of (2.2.3) is

$$Q_l = \frac{s^{l+1} - 1}{s - 1} \qquad \text{------- (2.2.4).}$$

It is clear that a 0 -flat is identical with a point , 1 -flat with line i.e. two independent points , a 2 -flat with plane i.e. three independent points, and so on.

Now we find the number of l -flats in PG(m,s).

It is clear that, each l -flat is determined by any set of $(l+1)$ independent points lying on it. Hence the total number of l - flats in PG(m,s) is equal to the number of ways of selecting $(l+1)$ independent points from the PG(m,s) divided by the number pf ways of selecting $(l+1)$ independent points on an l - flat. And it is denoted by $q(m,l,s)$.

Out of Q_m points, the first point can be chosen in Q_m ways and second in $Q_m - 1 = Q_m - Q_0$ ways. The third point must be chosen in such a way that it is linearly independent of the first two points, i.e. it should not be a point on the 1 -flat formed by the first two points. As, there are Q_1 points on a 1 -flat hence, the number of ways of choosing a third point is $Q_m - Q_1$. In general, the number of ways of choosing $(l+1)$ th point, having chosen l independent points and it is linearly independent of the first l points is $Q_m - Q_{l-1}$. Where Q_{l-1} are the points on $(l-1)$ -flat. Hence, the total number of ways of selecting $(l+1)$ independent ways in PG(m,s) are

$$Q_m (Q_m - Q_0)(Q_m - Q_1) --- (Q_m - Q_{l-1}) \quad ----(2.2.5)$$

But the same l -flat can be generated by any one of $Q_l (Q_l - Q_0)(Q_l - Q_1) --- (Q_l - Q_{l-1})$ sets of $(l+1)$ independant points. Therefore the total number of distinct l -flats in PG(m,s) is

$$Q(m,l,s) = \frac{Q_m (Q_m - Q_0) --- (Q_m - Q_{l-1})}{Q_l (Q_l - Q_0) --- (Q_l - Q_{l-1})} \quad \_\_\_\_\_\_(2.2.6)$$

Making the use of equation (2.2.2) and solving further, we get

$$Q(m,l,s) = \frac{(s^{m+1} - 1)(s^m - 1)(s^{m-1} - 1) --- (s^{m-l+1} - 1)}{(s^{l+1} - 1)(s^l - 1)(s^{l-1} - 1) --- (s - 1)}$$

----(2.2.7)

Remark :-

1. By using equation (2.2.5) we have

$$Q(m,l,s) = Q(m, m-l-1, s) \quad ------ (2.2.8)$$

2. $Q(m,0,s) = \dfrac{s^{m+1} - 1}{s - 1}$

Which is equal to number of points in PG(m,s). Hence, number of 0 -flats is equal to the number of points in PG(m,s).

Example 2.2.2 :- For PG(3,2) we find the number of points in PG(3,2) and number of 2 -flats. The number of points in PG(3,2)

$$Q_3 = \frac{2^{3+1} - 1}{2 - 1} = 15 .$$

And these are enumarated as ,

(0 0 0 1), (0 0 1 0), (0 0 1 1), (0 1 0 0), (0 1 0 1),
(0 1 1 0), (0 1 1 1), (1 0 0 0), (1 0 1 0), (1 0 1 1),
(1 1 0 0), (1 1 0 1), (1 1 1 0), (1 1 1 1), (0 0 0 0).

Further, number cf 2 -flats in PG(3,2) are given as ,

$$Q(3,2,2) = \frac{(2^4 - 1)(2^3 - 1)(2^2 - 1)}{(2^3 - 1)(2^2 - 1)(2^1 - 1)}$$

$$= 15 .$$

And these flats are ccnstituted by the solutions of following equations --

$$x_0 = 0 , \quad x_1 = 0 , \quad x_2 = 0 , \quad x_3 = 0 .$$

$$x_0 + x_1 = 0 , \quad x_1 + x_2 = 0 , \quad x_0 + x_1 + x_2 = 0 ,$$

$$x_0 + x_2 = 0 , \quad x_1 + x_3 = 0 , \quad x_0 + x_1 + x_3 = 0 ,$$

$$x_0 + x_3 = 0 , \quad x_2 + x_3 = 0 , \quad x_0 + x_2 + x_3 = 0 ,$$

$$x_1 + x_2 + x_3 = 0 \quad \text{and} \quad x_0 + x_1 + x_2 + x_3 = 0 .$$

Further , we get number of independant points in 2 -flats of PG(3,2) equal to

$$\frac{2^3 - 1}{2 - 1} = 7 .$$

If we take the intersecticns of pairs of 2 -flats , we obtain the design for 1 -flats . Number of 1 -flats are calculated as ;

$$Q(3,1,2) = \frac{(2^4 - 1)(2^3 - 1)}{(2^2 - 1)(2 - 1)} = \frac{15 \times 7}{3 \times 1} = 35 .$$

And number of points in each 1 -flat is ,

$$Q_1 = \frac{2^2 - 1}{2 - 1}$$

$$= 3 .$$

If we remove from PG(m,s) all the points in the (m - 1) dimensional subspace $x_0 = 0$, we can get a geometry , called as finite Euclidean geometry , denoted by EG(m,s). It can be described as follows --

2.3 The Finite Euclidean Geometry EG(m,s) :-

Any ordered set of m elements (x_1, x_2, - - x_m) belonging to GF(s) may be called a point of the finite m -dimensional Euclidean Geometry EG(m,s) , where the two points (x_1, x_2, - - - , x_m) and (y_1, y_2, - - - , y_m) are identical if and only if $x_i = y_i$; $i = 1, 2, 3, - - - , m$. It is clear that the number of points in EG(m,s) is s^m where $s = p^n$.

Definition 2.3.1 : 1 -flat :--

All the points satisfying a set of (m - 1) , (1 < m) consistent and independent linear equations --

$$\left.\begin{array}{l} a_{10} + a_{11} x_1 + a_{12} x_2 + - - - + a_{1m} x_m = 0 \\ a_{20} + a_{21} x_1 + a_{22} x_2 + - - - + a_{2m} x_m = 0 \\ - \\ - \\ - \\ a_{m-1,0} + a_{m-1,1} x_1 + - - - a_{m-1,m} x_m = 0 \end{array}\right] \quad ---(2.3.1)$$

may be said to constitute a 1 -flat of EG(m,s) represented by the equations(2.3.1).Any other set of m -1 consistent and independent linear equations which are obtained by linear combinations of(2.3.1) represent the same 1 -flat. The number of 1 -flats in EG(m,s) is

$$(m, 1, s) - (m-1, 1, s). \quad ----(2.3.2) .$$

Example 2.3.1 :-

Consider EG(3,2). Here m = 3 and s = 2 . Number of points in EG(3,2) is 2^3 = 8. And these are (0, 0, 0), (1,0,0), (0,1,0), (1,1,0), (0,0,1), (1,0,1), (0,1,1), (1,1,1). To obtain the 1 -flat we have to solve the equations - say

$x_1 = 0$ and $x_2 = 0$ simultaneously. And number of 1 -flats are --

$$Q (3,1,2) -- Q (2,1,2)$$

Now,

$$Q(2,1,2) = \frac{(2^4 - 1)(2^3 - 1)}{(2^2 - 1)(2 - 1)} = \frac{15 \times 7}{3 \times 1} = 35 .$$

and

$$Q(2,1,2) = \frac{(2^3 - 1)(2^1 - 1)}{(2^2 - 1)(2 - 1)} = \frac{7 \times 3}{3 \times 1} = 7 .$$

By substraction , we get number of 1 -flats equal to 28.

Relation between PG(m,s) and EG(m,s).

If $x_0 \neq 0$, then a point in PG(m,s) can be regarded as $(1, x_1/x_0, x_2/x_0, ---, x_m/x_0)$. A (m-1) -flat satisfying is called an (m-1) -flat at infinity , and points lying on it ed as points at infinity.

And the remaining points are called as finite points of PG(m,s).

If $x_0 \neq 0$, then point in PG(m,s) can be written as $(1, x'_1, x'_2, --- x'_n)$. where $x'_i = \frac{x_i}{x_0}$,i=1,2,- ,n. So there is 1:1 corrospondance between the finite points of PG(m,s) and the points $(x_1, x_2, ---, x_m)$ of EG(m,s). For any finite 1 -flat of PG(m,s) , given by

$$a_{10} x_0 + a_{11} x_1 + --- + a_{1m} x_m = 0 , \quad i=1,2, -- ,m-1. \quad --(2.3.3)$$

and corrosponding 1 -flat of EG(m,s) , given by the equation

$$a_{10} + a_{11} x_1 + --- + a_{1m} x_m = 0 , \quad i=1,2, -- ,m-1 . \quad ---(2.3.4)$$

It is easy to see that the set (2.3.4) is consistent when the

1 -flat of PG(m,s) is finite. Thus there is 1:1 corrospondance between finite 1 -flats in PG(m,s) and 1 -flats in EG(m,s), also the finite points on the 1 -flats of PG(m,s) corrospond to the points of the 1 -flats in EG(m,s). Thus by cutting all the points at $x_0 = 0$ and 1 -flats lying at infinity, EG(m,s) can be derived from PG(m,s). And by considering the points on EG(m,s) as the finite points of PG(m,s) and adding (m - 1) -flat at infinity at $x_0 = 0$, along with distinct points lying on it. We get PG(m,s) from EG(m,s).

We refer the two examples 2.2.1 and 2.2.2 and compare. In PG(3,2), the number of distinct points are

$$Q_3 = \frac{5^4 - 1}{5 - 1} = 15 .$$

And in EG(3,2) , these are $2^3 = 8$. And these points in EG(3,2) are obtained by discarding the points lying on 2 -flat of PG(m,s) represented by the equation $x_0 = 0$. i.e. the points (0,0,0,1), (0,0,1,0), (0,0,1,1),(0,1,0,0) and (0,1,0,1). Hence number of points in EG(3,2) = 15 - 7 = 8 .

=*=*=*=*=*=*=*=

==*=*=*

=*=