

An analysis of linear permutations contained in S_7 .

The general linear group of a vector space V finite field F will be contained in S_{n-1} where n is a power of p and p is the characteristic of F . Then $n = p^k$ where $k = i \cdot j$ and i is the dimension of V over F and j is the dimension of F over $GF(p)$. Of course, not all elements of S_{n-1} are linear.

If $t \in S_{n-1}$ is a linear permutation, $t \neq I$ (the identity permutation), and B is a basis of V , then there must be at least one element $v \in B$ such that $t(v) \neq v$, for if t fixes any basis of V it must fix all of V .

Let Q be an arbitrary subset of V . How large must Q be to guarantee that it contains at least one basis of V ? Of course this depends on the size of F , which is p^j and the dimension of V , which is i . Suppose that Q contains a linearly independent subset R and that $\|R\| = m < i$. Assume further, that Q contains no linearly independent subset larger than R . If this is the case, then every element of Q must be a linear combination of elements of R , for if there is an element $w \in Q$ that is not a linear combination of the elements of R , then $R \cup \{w\}$ is a linearly independent set larger than R . The number of linear combinations of elements of R is p^{jm} . Thus Q can contain at most p^{jm} vectors. If we insist that $0 \notin Q$, then Q can contain at most $p^{jm} - 1$ vectors, since the zero vector is a linear combination of any set of vectors.

Now consider the set of all non-singular 3×3 matrices over $GF(2)$. These matrices are all elements of S_7 .

Note that:

$$V = GF(2)^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$$

By the above reasoning, any set of 4 non-zero matrices must contain a basis of V , so every 3×3 matrix must move at least four points. Expressed in cycle form, all matrices, except the identity, have one of the following forms: $(v_1, v_2)(v_3, v_4)$ (Order 2), $(v_1, v_2, v_3)(v_4, v_5, v_6)$ (Order 3), $(v_1, v_2)(v_3, v_4, v_5, v_6)$ (Order 4), or $(v_1, v_2, v_3, v_4, v_5, v_6, v_7)$ (Order 7). Obviously, all order 2's are conjugate, as are all order 3's and all order 4's. Surprisingly, the order 7's fall into two distinct conjugate sets. The reason for this is that all order 2's have the same eigen polynomial, namely $x^3 + x^2 + x + 1$. All order 3's have the eigen polynomial, $x^3 + 1$. All order 4's have the eigen polynomial, $x^3 + x^2 + x + 1$, but order 7's may have either $x^3 + x^2 + 1$ or $x^3 + x + 1$, both of which are irreducible.

Eigenpolynomials for 4x4 GF(2) matrices

Let V be an n -dimensional vector space over $GF(2)$. Let T be a non-singular linear transformation from V to itself. The eigen polynomial of T must be of degree n . This

polynomial must be monic and must have a constant term of 1. (All polynomials over GF(2) are monic, and if the constant term were not 1, the eigen polynomial would have zero as a solution, making the linear transformation singular.)

The coefficients of the other $n-1$ terms are arbitrary, so there are 2^{n-1} polynomials that could serve as an eigen polynomial for T .

For 4×4 we have the following gallery.

Potential polynomials:

$$x^4 + 1 = (x+1)^4$$

$$x^4 + x + 1 = \text{irreducible}$$

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2$$

$$x^4 + x^2 + x + 1 = (x^3 + x^2 + 1)(x + 1)$$

$$x^4 + x^3 + 1 = \text{irreducible}$$

$$x^4 + x^3 + x + 1 = (x^2 + 1)(x^2 + x + 1)$$

$$x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1)$$

$$x^4 + x^3 + x^2 + x + 1 = \text{irreducible}$$

All of these are used as eigen polynomials for some class of transformations.

$$\text{Order 2 -- } x^4 + 1$$

$$\text{Order 3 -- } x^4 + x^2 + 1$$

$$\text{Order 4 -- } x^4 + 1$$

$$\text{Order 5 -- } x^4 + x^3 + x^2 + x + 1$$

$$\text{Order 6 -- } x^4 + x^2 + 1 \text{ or } x^4 + x^3 + x + 1$$

$$\text{Order 7 -- } x^4 + x^3 + x^2 + 1 \text{ or } x^4 + x^2 + x + 1$$

$$\text{Order 15 -- } x^4 + x + 1 \text{ or } x^4 + x^3 + 1$$

Other notes.

The order of the matrix is equal to the order of the eigen values, except when the order is a power of 2, in which case the eigen values are all one.

The order of the polynomial p is the smallest e such that p divides $x^e + 1$. The order of the eigen polynomial is equal to the order of the matrix.