***Galois Field Matrix’s Eigenvectors***

Author : Hyeong Rae Jo

Statement 1 : One eigenvector can only have one eigenvalue.

Proof :

Let A**v**=λ1**v**, A**v**=λ2**v**. than λ1**v** = A**v** = λ2**v**, λ1**v** = λ2**v**

Let k\*x ≡ k (mod p), 0<=k<=p-1, p is prime. Than gcd(k,p) is 1 for all k and p.

Since gcd(k,p) is 1, there is only one solution for x which is 1.

This means multiple of **v** is **v** when it is multiplied by only 1.

Thus λ1 is same as λ2 or λ2 - λ1 is multiple of p but this is impossible in Zp.

Hence, λ1 = λ2

Statement 2 : Let Null space of (A – λ1\*I) as N, and Null space of (A – λ2\*I) as M. if λ1 ≠ λ2 , then basis of N and M is mutually independent.

Proof :

Let **v**1,**v**2 to be any vector(except zero-vector) in N,M respectfully. Let’s see if **v**1 and **v**2 is independent.

Since **v**1,**v**2 can be any vector in N,M respectfully, if **v**1 and **v**2 is independent, we can conclude that basis of N and M is mutually independent.

Let a**v**1 = b**v**2. By multiplying (A – λ1\*I), we get a(A – λ1\*I)**v**1 = b(A – λ1\*I)**v**2.

Since (A – λ1\*I)**v**1 is zero-vector, b(A – λ1\*I)**v**2 is also zero-vector.

This means b(A**v**2 - λ1**v**2)=**0**, b(λ2**v**2 - λ1**v**2)=**0**.

Since λ1 and λ2 is different, b is 0 and so does a. this means **v**1 and **v**2 is independent. (statement 1)

Statement 3 : n \* n Galois Field Matrix A(GFMatrix for short) has maximum n eigenvalues and eigenvectors.

Proof :

Column or Row space of A has maximum dimension n.

Each eigenvalue can create Null space of dim n-rank. and it is minimum 1 which is just a line.

Since maximum dim is n, there are maximum n total eigenvalues.

This is true because Null spaces don’t overlap each other. (statement 2)

dim of each Null space is number of eigenvectors. So there are maximum n eigenvectors.

Statement 4 : Not all Galois Field Vector **v** (GFvector for short) can be normalized in any Zp except Z2.

Proof :

Only way to manipulate GFvector is multiplying some integer in Zp.

Let **v** = <v1,v2,v3,~,vn>, **u**=<v1/||**v**||,v2/||**v**||,~,vn/||**v**||> = <v1\*||**v**||-1, v2\*||**v**||-1,~,vn\*||v||-1>.

This means ||**v**|| must be able to be calculated from ||**v**||2.

Then ||**v**||\*||**v**|| should fill whole Zp because if not, certain ||**v**||2 cannot be factored into ||**v**||\*||**v**||.

Now let’s turn this to n\*n ≡ k (mod p). different n should make different k.

But this is not the case. Because think about n\*n,(n+1)\*(n+1)=n\*n+2n+1.

If 2n+1 is p, then n\*n ≡ (n+1)\*(n+1) (mod p). 2n+1 is odd number so it can be p.

Now we can conclude that not all GFvector can be normalized in any Zp except Z2.

(in Z2, every GFvector’s length is 1 or 0 because they are only possible numbers)

Statement 5 : Diagonalizable matrix has period of p-1.

Proof :

If matrix A is diagonalizable, then A=SDS-1. If D=I, A=SIS-1=SS-1=I.

Each diagonal component of D has order in Zp.

For example, in Z5, ord(3)=4. Because 3\*3\*3\*3=81, 81 mod 5 = 1.

Obviously maximum order is p-1. Because power of n can make p-1 number at most (except 0).

Let 1,2,3,~,p-1 to be Zp\*. Then order of any diagonal component of D can divide p-1 thanks to Lagrange's theorem about group theory.

LCM of each diagonal component of D is just p-1 and is also period of A. Because A^(p-1) =I.

In some cases, maximum of ord(diagonal component of D) is less than p-1. In this case, period might be smaller than p-1, but p-1 still works too.