Dimension Argument

UGTCS

February 4, 2019

1 Definitions

$GF(p^k)$ =Galois Field of Cardinaly p^k.

2 Random Matrices

Let M be an $n \times n$ matrix on $GF(2)$. Prove that $Pr[det(M) \neq 0] \geq \frac{1}{4}$

Proof. $det(M) \neq 0 \iff$ Every column is linearly indep.

Pr[each column is LI] $= \prod_i Pr[c_1, \cdots, c_i$ are LI $| c_1, \cdots, c_{i-1}$ are LI$]$ $c1, \cdots, c_{i-1}$ are LI iff sizeof(span($c_1, \cdots, c_{i-1}$)) $= 2^{i-1}$
$Pr[c_1, \cdots, c_i$ are LI $| c_1, \cdots, c_{i-1}$ are LI$] = 1 - \frac{2^{i-1}}{2^n}$
Use inequality:

$$a - x \geq 4^{-x} \forall x \in [0, 0.5]$$

$$\prod_{i=1}^{n} 1 - 2^{i-1-n} \geq \prod 4^{2^{i-1-n}} = 4^{-(2^{-1}+2^{-2}+\cdots+2^{-n})} \geq 4^{-1}$$

□

3 Polynomials

Prove a polynomial of degree d has $\leq d$ real roots using Linear Algebra.

Proof. Represent $c_0 x^0 + c_1 x^1 + \cdots$ as $[c_0, c_1, \cdots]\vec{c}$
If we have a root r, then $[1, r, r^2, \cdots] \cdot \vec{c} = \vec{0}$
For contradiction, assume $d+1$ roots $r_1, r_2, \cdots, r_{d+1}$, then

$$\rrbracket \llbracket = \vec{0}$$

Property of a Vandermonde Matrix V: $det(V) = \prod_{i \neq j}(\alpha_i - \alpha_j)$
Then the left matrix have all LI columns since no two roots are the same. □