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.

$Pr[\text{each column is LI}] = \prod_i Pr[c_1, \cdots, c_i \text{ are LI} \,|\, c_1, \cdots, c_{i-1} \text{ are LI}]$ $c1, \cdots, c_{i-1}$ are LI iff sizeof(span$(c_1, \cdots, c_{i-1})) = 2^{i-1}$
$Pr[c_1, \cdots, c_i \text{ are LI} \,|\, c_1, \cdots, c_{i-1} \text{ are LI}] = 1 - \frac{2^{i-1}}{2^n}$
Use inequality:
$$a - x \geq 4^{-x} \forall x \in [0, 0.5]$$

$\square$