Rank of Random Matrices over Finite Fields

Picture of an instantiation of a random matrix, color coded

Amin Shokrollahi
EPFL

Problem

m, n positive integers

$\mathcal{D}$ probability distribution on $\mathbb{F}_q^{m \times n}$

$X \sim \mathcal{D}$

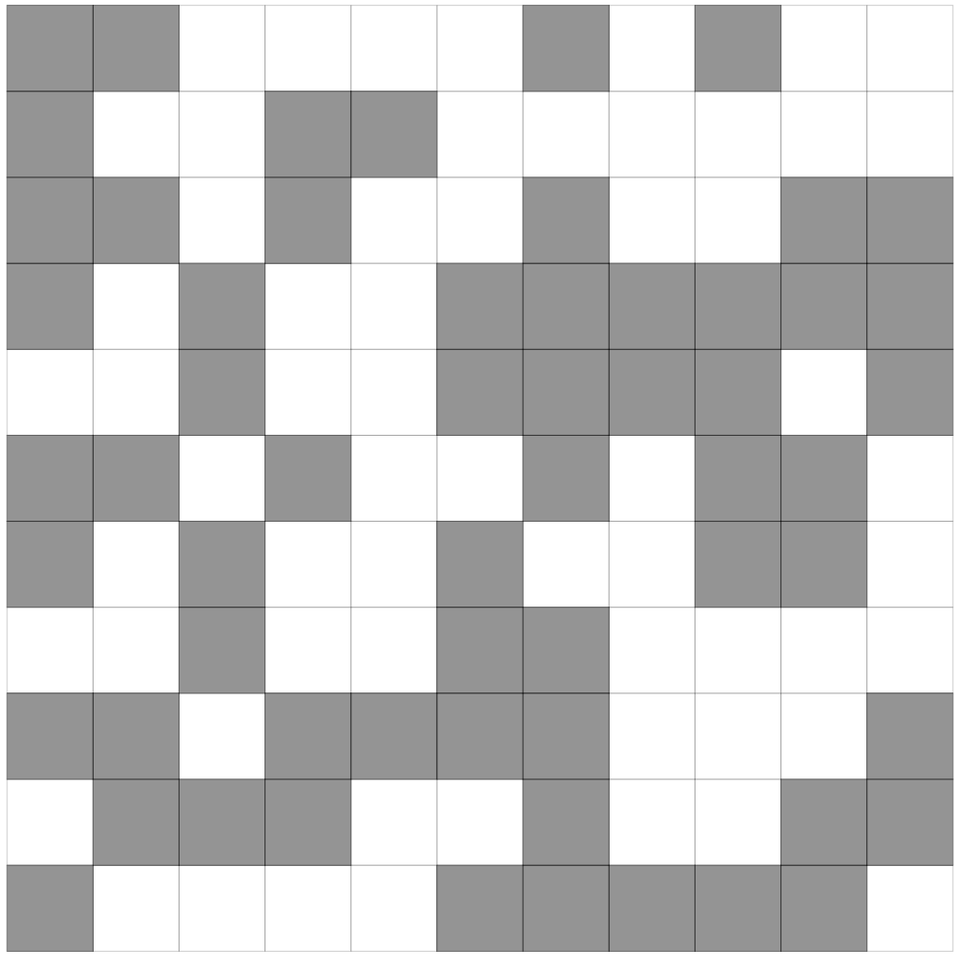
$$\Pr[\mathrm{rk}(X) = m]$$

$$\Pr[\mathrm{rk}(X) = k]$$
$$1 \leq k \leq m$$

Example

$\mathcal{D}$ uniform distribution on $\mathbb{F}_2^{m \times n}$

Every entry is independently chosen to be 1 with prob 0.5



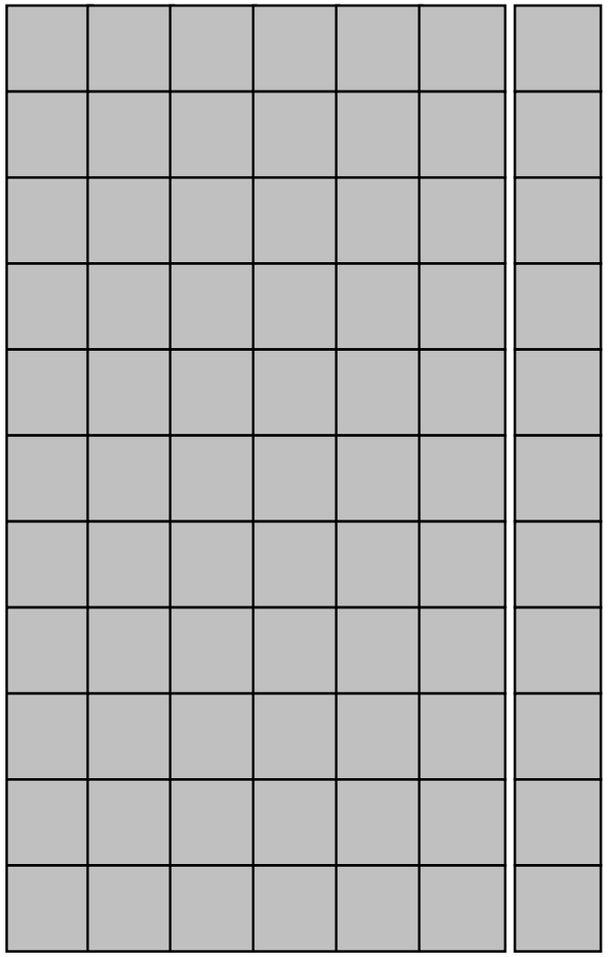
Dynamic Programming

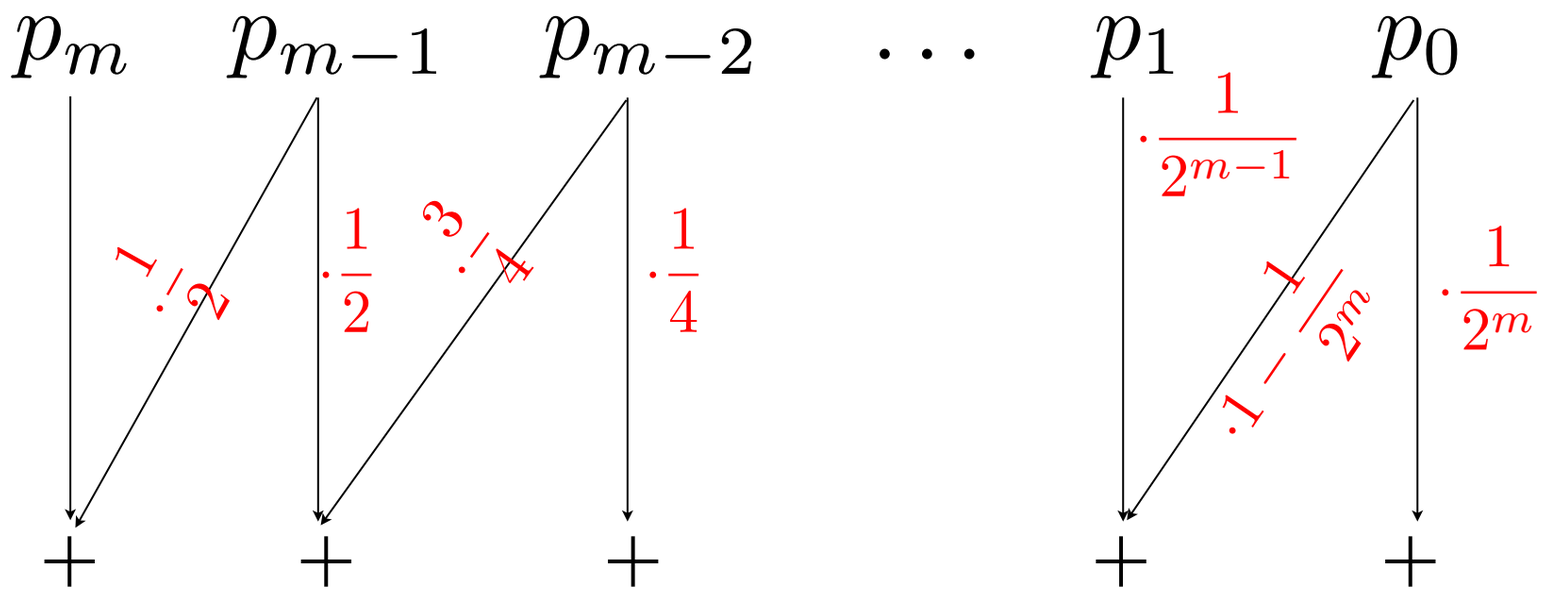
$p_i := \Pr[\mathrm{rk}(X) = i]$

Rank profile: $(p_m, p_{m-1}, \ldots, p_0)$

Add columns one at a time, evolve rank profile

Dynamic Programming





Dynamic Programming

$$\begin{pmatrix} p_m \\ p_{m-1} \\ p_{m-2} \\ \vdots \\ p_1 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} & 0 & \cdots & 0 & 0 \\ 0 & \frac{1}{2} & \frac{3}{4} & \cdots & 0 & 0 \\ 0 & 0 & \frac{1}{4} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{1}{2^{m-1}} & 1-\frac{1}{2^m} \\ 0 & 0 & 0 & \cdots & 0 & \frac{1}{2^m} \end{pmatrix}^n \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Possible to get approximative analytic expressions

Sparser Matrices

Uniform distribution is not sparse.

Fix $0 \leq p \leq 1$. Each entry is independently 1 with prob p.

Fix $0 \leq p \leq 1$. Each entry is independently nonzero with prob p. If nonzero, then every nonzero element of $\mathbb{F}_q$ appears with equal probability.

Picture goes here

Sparser Matrices

Previous method does not work.

Upper bounds on probability of rank deficiency

Method of Bloemer, Karp, Welzl: Union Bound

$$\begin{aligned}\Pr[\mathrm{rk}(X) < m] &= \Pr[\exists 0 \neq a \in \mathbb{F}_q^m : aX = 0] \\ &\leq \sum_{\mathbb{F}_q^m \ni a \neq 0} \Pr[aX = 0]\end{aligned}$$

Sparser Matrices

Biased distribution: 1 with prob p

Bloemer, Karp, Welzl

Kernel method

Higher moments: matrices over GF(4)

Examples

Other types of randomness:
matrices of fixed row weight
fewer rows than columns

Example: random multigraph
row-weight is 2
Full rank: no cycles
Matrix is cycle-free iff all components are trees
Erdoes-Renyi model of random graphs

Example: random multigraph
row-weight is 2
Full rank: no cycles
Matrix is cycle-free iff all components are trees
Erdoes-Renyi model of random graphs

Larger row weights kernel method Klochin's results

Larger row weights kernel method Klochin's results

Phase transition: one- or two-sided?

Phase transition: one- or two-sided?

What about the rank?
Phase transitions?
EXIT charts

What about the rank?
Phase transitions?
EXIT charts

What about the rank?
Phase transitions?
EXIT charts

What about the rank?
Phase transitions?
EXIT charts

Larger fields?

GF(q): prob for square matrices

Prob for rectangular matrices?

Applications:

Erasure coding in the random setting

Applications:

Erasure coding in the random setting

Applications:

Erasure coding in the random setting