Problems to Solve

Denote

- $\mathcal{S} = \mathbb{F}_2[z]$ as the ring of binary polynomials
- $\mathcal{S}^n$ as the set of polynomials in $\mathcal{S}$ that has degree no more than n, in particular, $\mathcal{S}^1 = \{0, 1, z, z+1\}$

Problems

1. **Probability of sigularity** Denote $\Pr(n)$ as the probaility of the presense of a zero determinant matrix, uniformly randomly selected from the set of all $n \times n$ matrices with entries in $\mathcal{S}$ (or even in $\{0, 1, z\}$). Characterize the probaility, show it converges to 1 quickly.

   Fact 10^4 simulation shows the above is true.

   Conjucture

   $$\Pr(n) = (\frac{1}{4} + o(1))^n$$

2. **Fast determinant** Fast approach to find (or detect if is 0) the determinant of a square matrix with entries in $\mathcal{S}^1$.

   Quasi-Gaussian Notice any row operation (addition) or row (column) permutation does not change the determinant of such matrices. Hence for a matrix M, we can reduce it to the form

   $$\begin{pmatrix} 1 & 0 & 0 & \dots \\ z & 0 & 0 & \dots \\ & 1 & 0 & \dots \\ & z & 0 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

   where the trapezoid above $1, z$ is all 0. Now by row, column permutations, M can be reduced to

   $$\begin{pmatrix} D_1 & \times \\ zD_2 & \times \end{pmatrix}$$

   where D_i is any binary diagonal matrix hence $\det D_i = 0$ if the diagonal is not all 1. Similarly now column operation will reduce the lower left corner into a binary permutation matrix, i.e. a binay matrix that has at most one 1 on each row. Then

   $$\det M = \det \begin{pmatrix} D_1 & \times \\ zD_2 & P \end{pmatrix}$$

3. Denote $\mathrm{Pr}_M(n)$ as the probability of the presense of an non-MDS matrix when uniformly selected from the set of all $n \times n$ matrices having their entries in $\mathcal{S}^1$. Characterize the probability and show it is bounded above.