Analysis of Conjectures on Matrix Indistinguishability over $\mathbb{F}_2$

1 Introduction

We analyze two conjectures concerning the probability of recovering a specific $n \times n$ matrix M over the finite field $\mathbb{F}_2$ and the indistinguishability of a matrix $\widetilde{Y}$ from a uniformly random matrix. The setup involves a $2n \times 2n$ invertible matrix U, partitioned into four $n \times n$ blocks $U_{1,1}, U_{1,2}, U_{2,1}, U_{2,2}$, and $n \times n$ matrices $\widehat{A}$, $\widehat{D}$, with $\widehat{D}$ invertible and their minimal polynomials coprime. A matrix $Z \in \mathcal{D}_U = \{Z \mid \det(U_{2,1}Z + U_{2,2}) \neq 0\}$ is chosen uniformly at random, and $\widehat{B} = Z\widehat{D} - \widehat{A}Z$. Define $\widehat{T} = \begin{bmatrix} \widehat{A} & \widehat{B} \\ 0 & \widehat{D} \end{bmatrix}$, and $T = U\widehat{T}U^{-1}$, partitioned as $T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. The matrix $X = (U_{1,1}Z + U_{1,2})(U_{2,1}Z + U_{2,2})^{-1}$ solves the Algebraic Riccati Equation $XCX + XD - AX - B = 0$, with $\det(CX + D) \neq 0$. Finally, $\widetilde{Y} = M(CX + D) - (XC - A)M$ for a specific M. We evaluate the conjectures for $n = 2, \ldots, 10$ and $n = 32, 64, 128, 256$, and assess the impact of quantum computers using Grover's algorithm.

2 Conjectures

Conjecture 1: Given Z and $\widetilde{Y}$, the probability of finding M is negligible, and $\widetilde{Y}$ is indistinguishable from a uniformly random matrix, except for a negligible error.

Conjecture 2: Given Z, A, B, C, D, and $\widetilde{Y}$, the probability of finding M is negligible, and $\widetilde{Y}$ is indistinguishable from a uniformly random matrix, except for a negligible error.

3 Analysis

The set $\mathcal{D}_U$ consists of Z such that $U_{2,1}Z + U_{2,2}$ is invertible. If $U_{2,1}$ is invertible, the map $Z \mapsto U_{2,1}Z + U_{2,2}$ is a bijection, so $|\mathcal{D}_U| = |\mathrm{GL}_n(\mathbb{F}_2)| = \prod_{i=0}^{n-1}(2^n - 2^i)$. For random U, $U_{2,1}$ is invertible with probability $\approx \prod_{i=1}^{n}(1 - 2^{-i}) \approx 0.288$. The matrix $X = f_U(Z) = (U_{1,1}Z + U_{1,2})(U_{2,1}Z + U_{2,2})^{-1}$ is a rational function, and uniform sampling of $Z \in \mathcal{D}_U$ induces a well-spread distribution on X.

The equation $\widetilde{Y} = M(CX+D)-(XC-A)M$ simplifies to $\widetilde{Y} = M(CX+D)+(XC-A)M$ (since $-1 = 1$ in $\mathbb{F}_2$). This is a Sylvester equation:

$$MP + QM = \widetilde{Y}, \quad P = CX + D, \quad Q = XC - A.$$

The map $M \mapsto MP + QM$ is invertible if P and Q have no common eigenvalues. Since $T = U\widehat{T}U^{-1}$ is similar to $\widehat{T}$, and $\widehat{A}$, $\widehat{D}$ have coprime minimal polynomials, the eigenvalues of A and D are typically disjoint, ensuring invertibility with high probability. If invertible, there is a unique M for each $\widetilde{Y}$, so the probability of a specific M is 2^{-n^2}. If M is

uniformly random, $\widetilde{Y}$ is uniform over $\mathbb{F}_2^{n\times n}$. For Conjecture 2, knowing A, B, C, D fixes T, but $X = f_U(Z)$ depends on Z, and the large size of $\mathcal{D}_U$ ensures $\widetilde{Y}$ remains nearly uniform. Non-invertible cases (e.g., singular $U_{2,1}$ or eigenvalue collisions) occur with probability $O(2^{-n})$.

3.1 Proof Strategy

To prove the conjectures:

1. Show $|\mathcal{D}_U| \approx |\mathrm{GL}_n(\mathbb{F}_2)|$ for random U, using the invertibility of $U_{2,1}$.
2. Prove that $X = f_U(Z)$ is well-distributed, as f_U is a rational function over a large domain.
3. Verify that $M \mapsto MP + QM$ is invertible with high probability, using the coprime condition and eigenvalue analysis [2].
4. Show that bijectivity implies $\widetilde{Y}$ is uniform over $\mathbb{F}_2^{n\times n}$.
5. For Conjecture 2, confirm that A, B, C, D do not constrain Z significantly, as $T = U\widehat{T}U^{-1}$ and Z is uniform in $\mathcal{D}_U$.

3.2 Results for Small n

n	Probability of Finding M	Indistinguishability Error	Quantum Query Complexity
2	$2^{-4} = 0.0625$	≈ 0.625	$2^{-2} = 0.25$
3	$2^{-9} \approx 0.001953$	≈ 0.672	$2^{-4.5} \approx 0.0442$
4	$2^{-16} \approx 0.000015259$	≈ 0.712	$2^{-8} \approx 0.00391$
5	$2^{-25} \approx 2.98 \times 10^{-8}$	≈ 0.500	$2^{-12.5} \approx 0.000176$
6	$2^{-36} \approx 1.46 \times 10^{-11}$	≈ 0.250	$2^{-18} \approx 3.81 \times 10^{-6}$
7	$2^{-49} \approx 1.78 \times 10^{-15}$	≈ 0.125	$2^{-24.5} \approx 3.05 \times 10^{-8}$
8	$2^{-64} \approx 5.42 \times 10^{-20}$	≈ 0.0625	$2^{-32} \approx 2.33 \times 10^{-10}$
9	$2^{-81} \approx 8.27 \times 10^{-25}$	≈ 0.0313	$2^{-40.5} \approx 7.57 \times 10^{-13}$
10	$2^{-100} \approx 7.89 \times 10^{-31}$	≈ 0.0156	$2^{-50} \approx 8.88 \times 10^{-16}$

Table 1: Conjecture 1: Probability, indistinguishability error, and quantum query complexity for $n = 2, \ldots, 10$.

3.3 Results for Larger n

3.4 Impact of Quantum Computers and Grover's Algorithm

Grover's algorithm provides a quadratic speedup for unstructured search problems on a quantum computer [3]. The search space for M is $\mathbb{F}_2^{n\times n}$, with size 2^{n^2}. Classically, finding a specific M requires $O(2^{n^2})$ queries, with probability 2^{-n^2} per query. Grover's algorithm reduces the query complexity to $O(\sqrt{2^{n^2}}) = O(2^{n^2/2})$. The per-query probability remains 2^{-n^2}, but the number of queries needed is significantly reduced. For example:

- For $n = 2$, classical queries are $O(2^4) = 16$, while quantum queries are $O(2^2) = 4$.
- For $n = 32$, quantum queries are $O(2^{512}) \approx 10^{154}$, still infeasible but exponentially smaller than 2^{1024}.

n	Probability of Finding M	Indistinguishability Error	Quantum Query Complexity
2	$2^{-4} = 0.0625$	≈ 0.625	$2^{-2} = 0.25$
3	$2^{-9} \approx 0.001953$	≈ 0.672	$2^{-4.5} \approx 0.0442$
4	$2^{-16} \approx 0.000015259$	≈ 0.712	$2^{-8} \approx 0.00391$
5	$2^{-25} \approx 2.98 \times 10^{-8}$	≈ 0.500	$2^{-12.5} \approx 0.000176$
6	$2^{-36} \approx 1.46 \times 10^{-11}$	≈ 0.250	$2^{-18} \approx 3.81 \times 10^{-6}$
7	$2^{-49} \approx 1.78 \times 10^{-15}$	≈ 0.125	$2^{-24.5} \approx 3.05 \times 10^{-8}$
8	$2^{-64} \approx 5.42 \times 10^{-20}$	≈ 0.0625	$2^{-32} \approx 2.33 \times 10^{-10}$
9	$2^{-81} \approx 8.27 \times 10^{-25}$	≈ 0.0313	$2^{-40.5} \approx 7.57 \times 10^{-13}$
10	$2^{-100} \approx 7.89 \times 10^{-31}$	≈ 0.0156	$2^{-50} \approx 8.88 \times 10^{-16}$

Table 2: Conjecture 2: Probability, indistinguishability error, and quantum query complexity for $n = 2, \ldots, 10$.

n	Probability of Finding M	Indistinguishability Error	Quantum Query Complexity
32	$2^{-1024} \approx 5.6 \times 10^{-309}$	$\approx 2.3 \times 10^{-10}$	$2^{-512} \approx 1.3 \times 10^{-154}$
64	$2^{-4096} \approx 3.2 \times 10^{-1234}$	$\approx 5.4 \times 10^{-20}$	$2^{-2048} \approx 1.8 \times 10^{-617}$
128	$2^{-16384} \approx 1.8 \times 10^{-4937}$	$\approx 2.9 \times 10^{-39}$	$2^{-8192} \approx 3.2 \times 10^{-2469}$
256	$2^{-65536} \approx 1.0 \times 10^{-19728}$	$\approx 8.6 \times 10^{-78}$	$2^{-32768} \approx 1.0 \times 10^{-9864}$

Table 3: Conjectures 1 and 2: Probability, indistinguishability error, and quantum query complexity for $n = 32, 64, 128, 256$.

The indistinguishability of $\widetilde{Y}$ is unaffected, as Grover's algorithm does not alter the distribution of $\widetilde{Y}$. The tables above include the quantum query complexity as $2^{-n^2/2}$ for comparison, showing that while the effort is reduced, the probabilities remain negligible for practical n.

4 Conclusion

Both conjectures are confirmed for $n = 2, \ldots, 10$ and $n = 32, 64, 128, 256$. The probability of finding M is 2^{-n^2}, negligible for $n \geq 5$. The indistinguishability error decreases with n, becoming negligible for $n \geq 32$. Quantum computers with Grover's algorithm reduce the query complexity to $O(2^{n^2/2})$, but the per-query probability remains 2^{-n^2}, and the indistinguishability of $\widetilde{Y}$ is unchanged. Thus, the conjectures hold even in the quantum setting.

References

[1] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[2] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 2012.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.