Problem 1. We choose three $n \times n$ matrices A, B, C randomly, that says we choose 0 and 1 randomly for every entries of A, B and C. Then we choose a column vector r that is n dimension. Please analyze the property of probability

$$P(AB \neq C \mid ABr = Cr)$$

.

Thought 1. *Firstly, let's think about the distribution of $AB - C$. It's very interesting that $AB - C$ is also randomly distributed in $F_2^{n\times n}$. We choose AB and we use a randomly chosen matrix C to "flip" AB, then we can get a randomly matrix $AB - C$.*
Let's define $D = AB - C$ and our problem becomes

$$P(D \neq 0 \mid Dr = 0)$$

We define some collections of matrices as following:

$$M_i = \{D \in F_2^{n\times n} \mid rank(D) = i\}$$

Then $M_i (0 \leq i \leq n)$ is a partition of $F_2^{n\times n}$. By the Bayes Formula, we have

$$\begin{aligned}
&P(D \neq 0 \mid Dr = 0)\\
=&\frac{P(D \neq 0 \textit{ and } Dr = 0)}{P(Dr = 0)}\\
=&\frac{\sum_{i=1}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}{\sum_{i=0}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}\\
=&\frac{\sum_{i=1}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}{P(D \in M_0)P(Dr = 0 \mid D \in M_0) + \sum_{i=1}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}\\
=&\frac{\sum_{i=1}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}{2^{n^2} + \sum_{i=0}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)}
\end{aligned}$$

For simplicity, define $p = \sum_{i=1}^{n} P(D \in M_i)P(Dr = 0 \mid D \in M_i)$.
We know that

$$\sum_{i=1}^{n} P(D \in M_i) = 1 - 2^{n^2}$$

so there is a item satisfying $P(D \in M_i) \geq \frac{1-2^{n^2}}{n}$ *and the corresponding*

$$P(Dr = 0 \mid D \in M_i) = P(r \in Ker(D) \mid D \in M_i) = \frac{2^{n-rank(D)}}{2^n} = \frac{1}{2^i}$$

.
So $p > \frac{1-2^{n^2}}{n2^i} \geq \frac{1-2^{n^2}}{n2^n}$.
Finally, we can obtain our probability

$$P(D \neq 0 \mid Dr = 0) = \frac{p}{2^{-n^2} + p} > \frac{2^n}{2n + 2^n}$$

, which is very very close to 1.
It's very confusing because we think it should be a not so bad method to check the correction of a matrix multiplication. The reason that causes such a result is because that we choose the three matrices randomly, which cause the probability $P(AB = C)$ *is so small, that is* $\frac{1}{2^{n^2}}$. *In reality, when we want to check the correction of* $AB = C$*, such a probability should not so small.*

by dyy