Matrix Multiplication

In this question we will design a randomized algorithm to verify the answer of matrix multiplication efficiently. Given three $n \times n$ matrices A, B, C, we would like to verify whether $AB = C$ and our goal is to do it faster than computing AB. We consider the setting where A, B, C are all $\{0, 1\}$-matrices (each entry is 0 or 1) and all arithmetic operations are done modulo 2 (so $1 + 1 = 0$).

Here is an idea: pick a random n-dimensional vector r where each entry of r is 0 with probability $1/2$ and 1 with probability $1/2$. Argue that if $AB \neq C$, then $ABr \neq Cr$ with probability $1/2$. Use this to design a randomized algorithm for verifying matrix multiplication with error probability at most 0.0000001. Give a bound on the running time of your algorithm.

Interactive Proof

Suppose you have two coins that look exactly the same to you. But your friend John claims that one coin is actually a counterfeit. You ask him why, and he says that he cannot explain but he can just distinguish which is which. Design a randomized algorithm to test John with the following promises:

1. if John is honest, then you will trust him.
2. if John is lying, then you will catch him with probability 0.9999999.

Your algorithm can ask him a sequence of yes/no questions.