4. (Verifying matrix multiplication)

(a) Solutions:

i. The only type of error it can make is that there is non-zero elements, but the algorithm accepts it. For a worst case input, there is only one non-zero element in the matrix D of size $n \times n$. Denote this event as E Thus, the probability of this happening $Pr[E]$ satisfies $Pr[E] \leq (n^2-1)/n^2$. Thus the best upper bound of accepts an incorrect answer is $(n^2-1)/n^2$ for a worst case input.

ii. Since there only a one-sided error, we can use k repeated independent tests to amplify the probability. Denote error for this multirun test as E_m,

$$\begin{aligned} Pr[E_m] &= (P[E])^k && (1) \\ &\leq \left(\frac{n^2-1}{n^2}\right)^k && (2) \end{aligned}$$

Since we want to solve for lower bound, we can use the equality $1-x \leq e^{-x}$ and solve for a lower bound fo k, with $(1-1/n^2)^k \leq (e^{-1/n^2})^k \leq 1/3$. The obtained lower bound is $(\ln 3)n^2$.

iii. For each run, we need to calculate D_{ij}, which is $O(n)$ due to the way how inner product works. And we need to do at least $(\ln 3)n^2$ runs, thus the total run time or this algorithm is n^3.

(b)

Proof. The only difference between the classroom case and this case we want to prove is the last step, when we select this random vector $\bar{r}$ sequentially. Assuming in the worst case, the element D_{ij} is non-zero. Let's select r_j last after selecting all other elements. If $A \cdot B = C$, then the probability $Pr[AB\bar{r} = C\bar{r}]$ is 1 no matter what r_j we choose. However, if D_{ij} is not zero, the probability $Pr[AB\bar{r} = C\bar{r}] \leq 1/2$ because when we select value of r_j from a uniform distribution of two values, the probability of selecting the only one possible value (which may not even exist) we select to make the equality true for this row is at most $1/2$. Similarly, in our case, since we are choosing values from v values $[0, 1, 2, ..., v-1]$ instead of two values, the probability of selecting the only possible value to make the quality holds is at most $1/v$, which is our new better bound than $1/2$.

(c) Solution: Denote the event that the multiplication equality is true is T and the event that the algorithm doesn't find any mistake after i runs is B_i. We know that $Pr[T] = Pr[\overline{T}] = 1/2$. For the first run of the test, we know that $Pr[B_1 \mid \overline{T}] \leq 1/v$ and $Pr[B_1 \mid T] = 1$. Thus, using Bayes' law, after the first run, the *posterior* probability is

$$\begin{aligned} Pr[T \mid B_1] &= \frac{Pr[T]Pr[B_1 \mid T]}{Pr[T]Pr[B_1 \mid T] + Pr[\overline{T}]Pr[B_1 \mid \overline{T}]} && (3) \\ &\geq \frac{1/2}{1/2 + 1/(2v)} = \frac{v}{v+1} && (4) \end{aligned}$$

Similarly for the second test, the *posterior* is $Pr[T \mid B_2] \geq \frac{v^2}{v^2+1}$. It is easy to show that after n runs without finding any mistake, the *posterior* $Pr[T \mid B_n] = \frac{v^n}{v^n+1}$.