1.11.9 Imperfect prime tester

Note to self: Get someone to verify $pr(B|A) = \epsilon^r$ is indeed correct.

Lemma Claim: Let $f(N)$ be a probabilistic algorithm that determines if a number N is prime with bounded error $pr(w) = \epsilon < \frac{1}{2}$. We claim the probability of error after r executions is:

$$pr(B|A) = \epsilon^r$$

where B is the event we get "yes" after r executions and A is the event N is prime.

Proof:

Each execution of the algorithm is mutually independent. Hence, the total probability of error after executing r times is:

$$\begin{aligned} pr(\text{Error after } r \text{ executions}) &= pr(\text{error})_1 \times pr(\text{error})_2 \times \ldots \times pr(\text{error})_r \\ &= \epsilon \times \epsilon \times \ldots \times \epsilon \\ &= \epsilon^r \end{aligned}$$

Main Claim: Let $f(N)$ be a probabilistic function that correctly outputs "yes" if N is prime. Otherwise, if N is composite, $f(N)$ outputs "yes" with a bounded error probability ϵ. The probability that N is not prime after r executions is:

$$pr(\text{N is prime}|f(N) \text{ outputs 'yes' } r \text{ times}) = \frac{\epsilon^r}{1+\epsilon^r}$$

Proof: Let A and B be events:

- A: The event N is not prime (i.e., N is composite)
- $\bar{A}$: The event N is prime
- B: "Yes," output of the algorithm given N after r executions.

We want to know the probability that N is composite given the fact the algorithm told us "yes" r times. Formally, we want $pr(A|B)$.

Bayes' rule tells us:

$$pr(A|B) = \frac{pr(A) \times pr(B|A)}{pr(B)}$$

First, we find the denominator using the total probability:

$$pr(B) = pr(A)pr(B|A) + pr(\bar{A})pr(B|\bar{A})$$

We also know that $f(N)$ will always correctly output "yes" if N is indeed prime. So $pr(B|\bar{A}) = 1$. We also know by Lemma 1 $pr(B|A) = \epsilon^r$. Thus:

$$pr(B) = pr(A)\epsilon^r + pr(\bar{A})$$

Denote $p = pr(\bar{A}) = pr(A)$.

$$\begin{aligned} pr(B) &= p\epsilon^r + p \\ &= p(\epsilon^r + 1) \end{aligned}$$

Plugging back into Bayes' rule:

$$\begin{aligned} pr(A|B) &= \frac{pr(A) \times pr(B|A)}{pr(B)} \\ &= \frac{pr(A) \times pr(B|A)}{p(\epsilon^r + 1)} \\ &= \frac{p \times \epsilon^r}{p(\epsilon^r + 1)} \\ &= \frac{\epsilon^r}{\epsilon^r + 1} \end{aligned}$$

Therefore, we have shown $pr(A|B) = \frac{\epsilon^r}{\epsilon^r+1}$.