Algo PSet5 Q1

Stephen Chin

Fall 2019

Miller-Rabin-k

Given:

$$
\begin{aligned}
Nprime &= \text{N is prime} \\
Ncomp &= \text{N is composite} \\
Oprob &= \text{Output is "N is probably prime"} \\
Onot &= \text{Output is "N is not prime"}
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{P}(Nprime) &= \frac{1}{\log P} \\
\mathbb{P}(Ncomp) &= 1 - \mathbb{P}(Nprime) = 1 - \frac{1}{\log P} \\
\mathbb{P}(Onot \mid Nprime) &= 0 \\
\mathbb{P}(Oprob \mid Nprime) &= 1 \\
\mathbb{P}(Onot \mid Ncomp) &= 1 - 2^{-k} \\
\mathbb{P}(Oprob \mid Ncomp) &= 2^{-k}
\end{aligned}
$$

---

a)

$$\begin{aligned}
\mathbb{P}(\text{"Output N is prime"}) &= \mathbb{P}(Nprime \mid Oprob) \\
&= \frac{\mathbb{P}(Oprob \mid Nprime)\mathbb{P}(Nprime)}{\mathbb{P}(Oprob)} \\
&= \frac{\mathbb{P}(Oprob \mid Nprime)\mathbb{P}(Nprime)}{\mathbb{P}(Oprob \mid Nprime)\mathbb{P}(Nprime) + \mathbb{P}(Oprob \mid Ncomp)\mathbb{P}(Ncomp)} \\
&= \frac{1/\log P}{1/\log P + (2^{-k})(1 - 1/\log P)} \\
&= \frac{1/\log P}{1/\log P + 2^{-k} - 2^{-k}/\log P} \\
&= \frac{2^k/\log P}{2^k/\log P + 1 - 1/\log P} \\
&= \frac{2^k}{2^k + \log P - 1} \geq \frac{2^k}{2^k + \log P}
\end{aligned}$$

Thus, the probability that the output N is prime is at least $\frac{2^k}{2^k+\log P}$ where $\log P$ is the natural logarithm of P.

b)

$$\begin{aligned}
\frac{2^k}{2^k + \log P} &\geq 0.99 \\
2^k &\geq 0.99 * 2^k + 0.99 * \log P \\
2^k - 0.99 * 2^k = 0.01 * 2^k &\geq 0.99 \log P \\
2^k &\geq 99 \log P \\
k &\geq \log_2(99 \log_e P)
\end{aligned}$$

Thus, in order to be at least 99% sure that the output N is prime, k must be at least $\log_2(99 \ln P)$.