How Many Repetitions?

Andreas Klappenecker

Texas A&M University

Problem

Suppose that we have a randomized Monte Carlo algorithm that succeeds with probability

$$\frac{1}{p(n)},$$

where $p(n)$ is some polynomial in the length of the input.

Question

How many times do we need to repeat the algorithm to get success with high probability (meaning with probability approaching 1)?

Main Tool

Useful Inequality

$$1 + x \leqslant e^x.$$

Consider the function $f(x) = e^x - 1 - x$. Our inequality is equivalent to $f(x) \geqslant 0$, so our goal will be to prove that.

The function $f(x)$ has the derivative $f'(x) = e^x - 1$.

We have $f'(x) = 0$ if and only if $x = 0$.

The function $f(x)$ has a (global) minimum at $x = 0$, since $f''(0) = e^0 = 1 > 0$. We can conclude that $f(x) \geqslant f(0) = 0$.

Consequence

Corollary

Consequently, for all positive integers n, we have

$$\left(1+\frac{x}{n}\right)^n \leqslant (e^{x/n})^n = e^x.$$

Corollary

Let $p(n)$ be a polynomial in n. For all positive integers n, we have

$$\left(1-\frac{1}{p(n)}\right)^{p(n)} \leqslant (e^{-1/p(n)})^{p(n)} = e^{-1}.$$

Number of Repetions

Corollary

Let $p(n)$ be a polynomial in n. For all positive integers n, we have

$$\left(1 - \frac{1}{p(n)}\right)^{p(n)\ln n} \leqslant (e^{-1/p(n)})^{p(n)\ln n} = e^{-\ln n} = \frac{1}{n}.$$

Conclusion

Thus, if we repeat an algorithm that succeeds with probability $1/p(n)$ for $p(n)\ln n$ times, then we get with high probability a correct result.