10.11 First, we show a useful variant of the Chernoff bound. Let $\exp(x) = e^x$. Let $E(X)$ be the expectation of the random variable X. The Markov inequality says the following:

$$\Pr[X \geq t] \leq \frac{E(X)}{t}$$

The proof of this inequality is very simple: we use Σ if X is a discreet random variable, and $\int$ if it is a continuous random variable. For example,

$$\begin{aligned} E(X) &= \sum_i x_i \Pr[X = x_i] = \sum_{x_i < t} x_i \Pr[X = x_i] + \sum_{x_i \geq t} x_i \Pr[X = x_i] \geq t \sum_{x_i \geq t} \Pr[X = x_i] \\ &= t \Pr[X \geq t] \end{aligned}$$

The Chernoff bound works for random variables that are sums of independent trials (so called Poisson trials). Thus, if $X_1, X_2, \ldots, X_n$ are independent Poisson trials with $\Pr[X_i = 1] = p_i$ (and thus $\Pr[X_i = 0] = 1 - p_i$), then $X = \sum_{i=1}^n X_i$ would be a random variable to which we can apply the Chernoff bound. If $p_i = p$ for all i, this special case is called Bernoulli trials, and the most common example is tossing a coin. Let $\mu = E(X)$, and for any $\delta \in (0, 1]$, we have the following Chernoff bound:

$$\Pr[X < (1 - \delta)\mu] < \left(\frac{e^{-\delta}}{(1 - \delta)^{(1-\delta)}} \right)^{\mu} \tag{2}$$

This can be simplified to two variants of the Chernoff bound which are easier to use:

$$\Pr[X < (1 - \delta)\mu] < \exp(-\mu\delta^2/2) \tag{3}$$

$$\begin{cases} \Pr[X > (1 + \delta)\mu] < 2^{-\delta\mu} & \text{if } \delta > 2e - 1 \\ \Pr[X > (1 + \delta)\mu] < \exp(-\mu\delta^2/4) & \text{if } \delta \leq 2e - 1 \end{cases} \tag{4}$$

We shall use (4) for this problem. The proof of (2) can be given with the Markov inequality. The proofs of the other variants follow from the main Chernoff inequality.

Now we turn to problem 10.11. There exists a real number c such that $\varepsilon_1 < c < \varepsilon_2$. Let M_k be a probabilistic TM which runs M k-times (M is the machine in the problem, called mistakenly in the first line B). M_k accepts a given input w iff at least ck outcomes where accepting.

We now bound the error (we are going to fix k to be something specific at the end). Suppose that $w \in C$, then:

$$\begin{aligned} &\Pr[M_k \text{ rejects } w] \\ &= \Pr[\text{less than } ck \text{ outcomes where accepting}] \\ &= \Pr[\text{more than } (1 - c)k \text{ outcomes where rejecting}] \\ &= \Pr[X > (1 - c)k] \end{aligned}$$

Here $X = \sum_{i=1}^k X_i$, where $X_i = 1$ iff the i-th run is incorrect, and 0 otherwise. Also, note that $\mu = E(X) \leq (1 - \varepsilon_2)k$ since there are k *independent* runs, and if $w \in C$, then from b. we see that the probability of error is at most $(1 - \varepsilon_2)$, thus

$$\begin{aligned} &\leq \Pr[X > (1 - \varepsilon_2)k] \\ &= \Pr[X > (1 + \delta)\mu] \end{aligned}$$

where $\delta > 0$ is such that $(1+\delta)\mu = (1-\varepsilon_2)k$, and note that δ depends *only* on ε_2, so it can be given independently of what k we choose at the end. Now, depending what δ we get, we employ one of the inequalities in (4). Whichever we use, we make k sufficiently large so that:

$$\leq \frac{1}{2}$$

A similar analysis will give as a k such that if $w \notin C$, then the probability of accepting is less than $\frac{1}{2}$. We take the bigger of the two k's to be the final k.