1. Assume that ZF set theory (the standard axiom system for mathematics) is sound. Let \( M \) be a Turing machine that, on input \( x \) in \( \{0,1\}^n \), first checks whether \( x \) (or any contiguous substring of \( x \)) encodes a ZF proof that ZF is inconsistent, and then runs for \( 3^n \) steps if so, and for \( 2^n \) steps otherwise.

(a) What is \( M \)'s asymptotic running time?

(b) Is \( M \)'s asymptotic running time provable in ZF? Why or why not?

2. Let \( L \) be a subset of \( 0,1^n \). Since \( L \) is finite, it is clear that \( L \) is regular. Nevertheless, by using a variant of Shannon’s counting argument, show that it is possible to choose an \( L \) so that any DFA that recognizes \( L \) must have \( \Omega(2^n) \) states.

3. Give a context-free grammar that generates the complement of the language \( L = \{ a^m b^n \mid m, n > 0 \} \).
Solutions

1. Assume that ZF set theory (the standard axiom system for mathematics) is sound. Let $M$ be a Turing machine that, on input $x$ in $\{0, 1\}^n$, first checks whether $x$ (or any contiguous substring of $x$) encodes a ZF proof that ZF is inconsistent, and then runs for $3^n$ steps if so, and for $2^n$ steps otherwise.

   (a) **What is $M$’s asymptotic running time?**
   Since we are assuming ZF set theory is sound, $x$ will not encode a proof that ZF is inconsistent. Thus, $M$ will run for $O(2^n)$ steps.

   (b) **Is $M$’s asymptotic running time provable in ZF? Why or why not?**
   If one could prove in ZF $M$’s asymptotic time, one prove ZF’s consistency in ZF. Since we assumed ZF is sound, by Gödel’s Theorem, we cannot prove its consistency.

2. Let $L$ be a subset of $0, 1^n$. Since $L$ is finite, it is clear that $L$ is regular. Nevertheless, by using a variant of Shannon’s counting argument, show that it is possible to choose an $L$ so that any DFA that recognizes $L$ must have $Ω(\frac{2^n}{n})$ states.

   There are $2^n$ $n$-bit strings. For each of those strings, a given language will either include it or not include it — thus, there are $2^{2^n}$ total possibilities for $L$.

   Consider a DFA with $T$ states. Each of these states can connect to any other state, which means that the total number of $T$-state DFA’s is approximately $T^T$. Since a DFA decides one particular language, by the pigeonhole principle, it must be the case that there are at least as many DFA’s as languages; in other words,

   $$2^{2^n} \leq T^T$$
   $$\log_2 2^{2^n} \leq \log_2 T^T$$
   $$2^n \leq T \log_2 T$$

   Plugging in $\frac{2^n}{n}$ for $T$ and performing the same approximations as used in Shannon’s argument, one can see that $T$ must indeed be $Ω(\frac{2^n}{n})$ for the inequality to hold.

3. **Give a context-free grammar that generates the complement of the language $L = \{a^m b^n \mid m, n > 0\}$**.

   Note that $L$ is a regular language, meaning its complement is regular. too. It is not hard to come up with a DFA for $L$, after which we can simply switch all accepting and non-accepting states to come up with a DFA for $\overline{L}$. Then, we can make a regular expression for $\overline{L}$ and from that come up with the following grammar:
\[ S \rightarrow \varepsilon \mid A \mid bC \mid ABaC \]
\[ A \rightarrow aA \mid \varepsilon \]
\[ B \rightarrow bB \mid \varepsilon \]
\[ C \rightarrow aC \mid bC \mid \varepsilon \]