submitted by: Maulik Chhetri, Mahiem Agrawal, Subigya Paudel

Exercise 1

On Input w

① Non deterministically partition w ~~a maximum of~~ at a maximum of n-1 places, ($|w| = n$)

② Check whether each partition ~~of~~ belongs to A.

③ If ~~the~~ all the partitions belong to A, accept. Else reject.

① Stage 1 implies that we are non deterministically generating strings with different partitions.

② Checking the partition membership in A is in polynomial time using a non-deterministic turing machine since $A \in NP$.

③ Therefore $A^* \in NP$. //

Exercise 2

~~On input integer s.~~

Before factorizing, let us give a simple language that belongs to NP.

$L = \{n \mid n \text{ has a factor}\}$.

L is in NP since the factor can be used as a certificate

Now,

On Input s integer s.

Exercise 2

On input s

① Nondeterministically generate the set of integers G such that $\forall$ elements $x \in G$, $x \leq s$, and $|G| < \frac{s}{2}$

② Check if all the integers are prime and the product of all integer is s.

③ If true accept, else reject.

If $P = NP$, then the following computation would be done in polynomial time in a deterministic single tape turing machine.

Exercise 3

Giving a verifier for PARTITION.

Input $\langle w, c \rangle$, $c = \langle B, C \rangle$

① Test whether the ~~set~~ B, C ~~is of~~ ~~dat~~ satisfies the following condition: $B \cup C = w$ and $\sum(w) = n$, $|B| = |C| = n$.

② Test whether $\sum_{b \in B} s(b) = \sum_{c \in C} s(c)$.

③ If both conditions pass, then accept. Else reject.

Ⓘ Determining decider.

$V_{PARTITION}$ is a decider since testing of the 1st and 2nd case will both terminate.

Ⓘ$\!$Ⓘ $V_{PARTITION}$ is verifier.

⇒ If $w \in$ PARTITION, then there exists disjoint subsets B and C such, $B \cup C = w$ and $\sum_{b \in B} s(b) = \sum_{c \in C} s(c)$. Therefore

setting C to $\langle B, C \rangle$, $\omega \cdot \langle w, c \rangle$ is accepted by the verifier VPARTITION.

(⇐) If there exist a c such that $\langle w, c \rangle$ is accepted by the verifier, then step 1 implies that

$B \cup C = \omega$, and $|B| + |k| = n$, when $|\omega| = n$. ~~step 2~~
$\Rightarrow$ disjoint

step 2 implies that $\sum_{b \in B} s(b) = \sum_{c \in C} s(c)$. $\Rightarrow$ Partition property.

Hence, $w \in$ PARTITION.

(⇒) Polynomial time.

Step 1, to test ~~whether~~ whether ~~$|B|+|C|$~~ $B \cup C = \omega$, and $|B| + |C| = |\omega|$, can be done in polynomial time.

Comparing each value of B in ω and a in ω will be bounded by $O(n^2)$, $n = |\omega|$. ✓

summing the ~~integers with~~ sizes will be done in $O(n)$. ✓

Hence it is in polynomial time.